Tesis Doctoral

Teoremas de modularidad para grupos unitarios

Guerberoff, Lucio

2011

UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

UNIVERSITE PARIS 7 DENIS DIDEROT
Institut de Mathématiques de Jussieu
École Doctorale Paris Centre

TEOREMAS DE MODULARIDAD PARA GRUPOS UNITARIOS

Tesis presentada para optar al título de
Doctor de la Universidad de Buenos Aires
en el área Ciencias Matemáticas y
Doctor de la Université Paris 7 Denis Diderot,
Especialidad Ecole Doctorale Sciences Mathématiques de Paris Centre.

Lucio Guerberoff

Directores de tesis: Dr. Michael Harris
Dr. Ariel Pacetti
Consejero de estudios: Dr. Ariel Pacetti

Buenos Aires, 2011.

Tú eres el Sol. El Sol hace esto. Tú eres la Tierra. La Tierra primero está aquí, y luego la Tierra se mueve alrededor del Sol. Y ahora... una explicación, que incluso gente sencilla como nosotros puede entender, sobre la inmortalidad.

János Valuska, Werckmeister harmóniák
(Béla Tarr)

A Alberto Guerberoff, mi padre

MODULARITY LIFTING THEOREMS FOR UNITARY GROUPS

The main part of this thesis is devoted to the proof of modularity lifting theorems for ℓ-adic Galois representations of any dimension satisfying a unitary type condition and a Fontaine-Laffaille condition at ℓ. This extends the results of Clozel, Harris and Taylor, and the subsequent work by Taylor. The proof uses the Taylor-Wiles method, as improved by Diamond, Fujiwara, Kisin and Taylor, applied to Hecke algebras of unitary groups, and results of Labesse on stable base change and descent from unitary groups to GL_n. Our result is an ingredient of the recent proof of the Sato-Tate conjecture, and has been applied to prove other modularity lifting theorems as well.

At the end of the thesis, we include an algorithmic approach to modularity of elliptic curves over imaginary quadratic fields

THÉORÈMES DE MODULARITÉ POUR GROUPES UNITAIRES

La partie principale de cette thèse est dévouée à la démonstration de théorèmes de modularité pour des représentations galoisiennes ℓ-adiques de n'importe quelle dimension satisfaisant une condition de type unitaire et une condition de type Fontaine-Laffaille en ℓ. Ces résultats généralisent le travail de Clozel, Harris et Taylor, et l'article ultérieur de Taylor. La démonstration utilise la méthode de Taylor-Wiles, dans sa version ameliorée par Diamond, Fujiwara, Kisin et Taylor, appliquée aux algèbres d'Hecke de groupes unitaires, et des résultats de Labesse sur le changement de base stable et le descent des groupes unitaires vers GL_n. Notre résultat est un ingrédient de la récente démonstration de la conjecture de Sato-Tate conjecture, et il a été utilisé également pour démontrer des autres théorèmes de modularité.

À la fin de la thèse, on inclut une approche algorithmique pour la modularité des courbes elliptiques sur les corps quadratiques imaginaires.

TEOREMAS DE MODULARIDAD PARA GRUPOS UNITARIOS

La parte principal de esta tesis está dedicada a la demostración de teoremas de modularidad para representaciones de Galois ℓ-ádicas de cualquier dimensión que satisfacen una condición de tipo unitario y una condición de Fontaine-Laffaille en ℓ. Esto extiende los resultados de Clozel, Harris y Taylor, y el trabajo subsiguiente de Taylor. La demostración utiliza el método de Taylor-Wiles, en su versión mejorada por Diamond, Fujiwara, Kisin y Taylor, aplicado a álgebras de Hecke de grupos unitarios, y resultados de Labesse sobre cambio de base estable y descenso de grupos unitarios a GL_n. Nuestro resultado es utilizado como ingrediente de la reciente demostración de la conjetura de Sato-Tate, y ha sido también aplicado para probar otros teoremas de modularidad.

En el final de esta tesis, incluimos un enfoque algorítmico para la modularidad de curvas elípticas sobre cuerpos cuadráticos imaginarios.

Agradecimientos/Acknowledgements/Remerciements

In the first place I would like to thank my thesis adviser Michael Harris for everything he has done over these years. He has teached me a lot of mathematics, and has transmitted to me many insightful views about the whole field, not only about this thesis. His advices and support are a very strong pillar of this thesis.

I also thank my co-adviser Ariel Pacetti, for all his advices, the mathematics conversations I had with him, and for being available all the time for what I needed.

I would also like to thank Roberto Miatello, whose continuous support and encouragement have been invaluable to me.

I would like to thank those mathematicians and colleagues with which I have mantained very fruitful conversations about mathematics. I mention Daniel Barrera Salazar, Nicolás Ojeda Bar, Fernando Cukierman, Hendrik Verhoek, Paul-James White, Mao Sheng, among others.

A nivel personal, agradezco a mi mujer, Andrea, que estuvo a mi lado como mi compañera durante todos estos años, y me apoyó en todos los aspectos a lo largo de este proceso. Agradezco también a mi mamá, Irene, que desde siempre me ayudó y apoyó con todo, alentándome a elegir mi propio camino. A mi hermana, Julieta, le agradezco haber estado conmigo siempre, en las buenas y en las malas. Por último, pero no menos importante, quiero agradecerle a mi papá, Alberto Guerberoff, quien me ayudó a formarme como persona, enseñándome una innumerable cantidad de cosas sobre la vida y otras yerbas, y a quien nunca dejo de extrañar. Es a él a quien esta tesis está dedicada.

Quiero agradecer también a la Profesora Alicia Dickenstein por su invaluable ayuda en la presentación de esta tesis. Finalement, je voudrais beaucoup remercier Mme. Douchez, Mme. Wasse et Mme. Dupouy pour le support administratif dans toutes les démarches de cette thèse.

Contents

Introduction

The most important object of study of algebraic number theory is the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$, or more generally, of a number field. According to the Tannakian philosophy, one should study the representations of these groups. Several years ago, with this in mind, Langlands stated a number of widescope conjectures relating objects from number theory, arithmetic algebraic geometry and representation theory, giving rise to what is now commonly known as the Langlands program. In this thesis we treat some particular problems embodied in this program, relating on one side Galois representations and on the other side automorphic representations.

The first part of this thesis is devoted to so-called modularity lifting theorems. Roughly speaking, the aim is to prove that if an ℓ-adic Galois representation $r : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ is such that its modulo ℓ reduction $\bar{r} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ is modular (or automorphic), that is, it comes from modular forms, then r itself is modular, assuming some additional hypotheses. The original idea is due to Wiles, leading him, along with Taylor, to the celebrated proof of Fermat's Last Theorem (**[Wil95, TW95]**). Here, we prove modularity lifting theorems for ℓ-adic Galois representations of any dimension satisfying certain conditions (**[Gue]**). We extend the results of **[CHT08]** and **[Tay08]**, where an extra local condition appears. In this work we remove that condition, which can be done thanks to the latest developments of the trace formula. More precisely, let F be a totally imaginary quadratic extension of a totally real field F^+. Let Π be a cuspidal automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$. We say that Π es *essentially conjugate self-dual* if there exists a continuous character $\chi : \mathbb{A}_{F^+}^\times/(F^+)^\times \to \mathbb{C}^\times$ such that $\chi_v(-1)$ is independent of $v|\infty$ and

$$\Pi^\vee \cong \Pi^c \otimes (\chi \circ \mathbf{N}_{F/F^+} \circ \det).$$

Here, c is the non-trivial Galois automorphism of F/F^+. If we can take $\chi = 1$ in this definition, we say that Π is *conjugate self-dual*. We also say that Π is *cohomological* if the archimedean component Π_∞ has the same infinitesimal character as an algebraic, finite dimensional, irreducible representation of $(\mathrm{Res}_{F/\mathbb{Q}} \mathrm{GL}_n)(\mathbb{C})$. Let ℓ be a prime number, and $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$ an isomorphism. Then there is a continuous semisimple Galois representation

$$r_{\ell,\iota}(\Pi) : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

which satisfies certain expected conditions. In particular, for places v of F not dividing ℓ, the restriction $r_{\ell,\iota}(\Pi)|_{\mathrm{Gal}(\overline{F}_v/F_v)}$ to a decomposition group at v should be isomorphic, as a Weil-Deligne representation, to the representation corresponding to Π_v under a suitably normalized local Langlands correspondence. The construction of the Galois representation $r_{\ell,\iota}(\Pi)$ under these hypotheses is due to Clozel, Harris and Labesse ([**CHLa, CHLb**]), Chenevier and Harris ([**CH09**]), and Shin ([**Shi11**]), although they only match the Weil parts and not the whole Weil-Deligne representation. In the case that Π satisfies the additional hypothesis that Π_v is a square integrable representation for some finite place v, the above construction is carried out by Harris and Taylor in [**HT01**], and Taylor and Yoshida have shown in [**TY07**] that the corresponding Weil-Deligne representations are indeed the same, as expected. Without the square integrable hypothesis, this is proved by Shin in [**Shi11**] in the case where n is odd, or when n is even and the archimedean weight of Π is 'slightly regular', a mild condition we will not recall here. This local-global compatibility was finally completed by Caraiani in [**Car10**].

We use the instances of stable base change and descent from GL_n to unitary groups, proved by Labesse ([**Lab**]), to attach Galois representations to automorphic representations of totally definite unitary groups. In this setting, we prove an $R^{\mathrm{red}} = T$ theorem, where R is a certain universal deformation ring and $\mathbb{T}$ is a unitary group Hecke algebra, following the development of the Taylor-Wiles method used in [**Tay08**]. Finally, using the results of Labesse again, we prove our modularity lifting theorem for GL_n. This generalizes the theorems proved in [**CHT08**] and [**Tay08**], where an extra local hypothesis is needed, reflecting the earlier construction of $r_\ell(\Pi)$ which requires Π_v to be square integrable for some finite place v. The removal of this condition also translates in the fact that we use untwisted unitary groups, as opossed to the twisted groups used in *loc. cit.* The most general theorem we prove for imaginary CM fields is the following. For the terminology used in the different hypotheses, we refer the reader to the main text.

THEOREM. *Let F^+ be a totally real field, and F a totally imaginary quadratic extension of F^+. Let $n \geqslant 1$ be an integer and $\ell > n$ be a prime number, unramified in F. Let*

$$r : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

be a continuous irreducible representation with the following properties. Let $\bar{r}$ denote the semisimplification of the reduction of r.

(i) $r^c \cong r^\vee(1-n)$.
(ii) r is unramified at all but finitely many primes.
(iii) For every place $v|\ell$ of F, $r|_{\Gamma_v}$ is crystalline.
(iv) There is an element $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,\overline{\mathbb{Q}}_\ell)}$ such that

- *for all $\tau \in \mathrm{Hom}(F^+, \overline{\mathbb{Q}}_\ell)$, we have either*

$$\ell - 1 - n \geqslant a_{\tau,1} \geqslant \cdots \geqslant a_{\tau,n} \geqslant 0$$

or

$$\ell - 1 - n \geqslant a_{\tau c,1} \geqslant \cdots \geqslant a_{\tau c,n} \geqslant 0;$$

- *for all $\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_\ell)$ and every $i = 1, \ldots, n$,*

$$a_{\tau c,i} = -a_{\tau,n+1-i}.$$

- *for all* $\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_\ell)$ *giving rise to a prime* $w|\ell$,

$$\mathrm{HT}_\tau(r|_{\Gamma_w}) = \{j - n - a_{\tau,j}\}_{j=1}^n.$$

In particular, r is Hodge-Tate regular.

(v) $\overline{F}^{\ker(\operatorname{ad}\overline{r})}$ *does not contain* $F(\zeta_\ell)$.

(vi) The group $\overline{r}(\mathrm{Gal}(\overline{F}/F(\zeta_\ell)))$ *is big.*

(vii) The representation $\overline{r}$ *is irreducible and there is a conjugate self-dual, cohomological, cuspidal automorphic representation* Π *of* $\mathrm{GL}_n(\mathbb{A}_F)$*, of weight* $\mathbf{a}$ *and unramified above* ℓ*, and an isomorphism* $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$*, such that* $\overline{r} \cong \overline{r}_{\ell,\iota}(\Pi)$.

Then r is automorphic of weight $\mathbf{a}$ *and level prime to* ℓ.

We make some remarks about the conditions in the theorem. Condition (i) says that r is conjugate self-dual, and this is essential for the numerology behind the Taylor-Wiles method. Conditions (ii) and (iii) say that the Galois representation is geometric in the sense of Fontaine-Mazur, although it says a little more. It is expected that one can relax condition (iii) to the requirement that r is de Rham at places dividing ℓ. The stronger crystalline form, the hypothesis on the Hodge-Tate weights made in (iv) and the requirement that $\ell > n$ is unramified in F are needed to apply the theory of Fontaine and Laffaille to calculate the local deformation rings. The condition that $\ell > n$ is also used to treat non-minimal deformations. Condition (v) allows us to choose auxiliary primes to augment the level and ensure that certain level structures are sufficiently small. The bigness condition in (vi) is to make the Tchebotarev argument in the Taylor-Wiles method work. Hypothesis (vii) is, as usual, essential to the method. An analogous theorem can be proved over totally real fields. The contents of this part correspond to the article [**Gue**]. We would like to mention that after this article was written, some of the conditions on the theorem were relaxed by further works. Important improvements include the relaxation of the condition that ℓ is unramified in F ([**BLGG11**]) and the weakening of the troublesome 'bigness' conditions ([**Tho10**]). A recent source combining all known results up to date is [**BLGGT10**].

In the second part of this thesis, we adopt an algorithmic approach to prove modularity for a given elliptic curve E over an imaginary quadratic field F ([**DGP10**]). The algorithm is based on the Faltings-Serre method, which serves to compare two ℓ-adic Galois representations. In our case, let $r_2(E) : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{Z}_2)$ be the continuous 2-adic representation of the Galois group of F given by the action on the 2-adic Tate module of E, and denote by $\overline{r_2(E)} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{F}_2)$ the residual representation. We assume that E does not have complex multiplication, so that $r_2(E)$ is absolutely irreducible. If Π is a cohomological cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ with unitary central character, there is attached to it a Galois representation $r_2(\Pi) : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_2)$ ([**HST93, Tay94, BH07**]). The Faltings-Serre method, as used in our paper, provides a finite list $\{v_1, \ldots, v_m\}$ of primes of F with the property that if $\mathrm{Tr}(r_2(E)(\mathrm{Frob}_{v_i})) = \mathrm{Tr}(r_2(\Pi)(\mathrm{Frob}_{v_i}))$ for $i = 1, \ldots, m$, then $r_2(E)$ and $r_2(\Pi)$ are isomorphic.

Our use of the Faltings-Serre method is divided into cases according whether the image of $\overline{r_2(E)}$ is trivial, cyclic of order 2, cyclic of order 3, or the whole group $\mathrm{GL}_2(\mathbb{F}_2)$. By an argument given by Taylor in **[Tay94]**, we can choose two split primes v_1 and v_2 for which if $\mathrm{Tr}(r_2(E)(\mathrm{Frob}_{v_i})) = \mathrm{Tr}(r_2(\Pi)(\mathrm{Frob}_{v_i}))$ for $i = 1, 2$, then the representation $r_2(\Pi)$ can be taken to have values in $\mathrm{GL}_2(L)$, where L is a finite extension of $\mathbb{Q}_2$ with residue field $\mathbb{F}_2$. Actually we search for the first two primes such that 2 has no inertial degree on the field obtained by adding to $\mathbb{Q}$ the roots of the Frobenius characteristic polynomials. We thus include first these two primes in our output of the algorithm, and if the traces of Frobenius do not coincide on some of these primes, then obviously the representations will not be isomorphic and the comparison is finished. Suppose now that indeed the traces of Frobenius at these two primes are the same. According to each case of the possible images of $\overline{r_2(E)}$, we find, ussing class field theory, a finite list of primes such that if the traces of Frobenius agree at these primes, then the residual image of $r_2(\Pi)$ will also be the same as that of $\overline{r_2(E)}$. For example, if the image of $\overline{r_2(E)}$ is cyclic of order 3 or $\mathrm{GL}_2(\mathbb{F}_2)$, then elements of this group of order 1 or 2 have even trace, and thus it suffices to find a prime v for which $\mathrm{Tr}(r_2(E)(\mathrm{Frob}_v)) = \mathrm{Tr}(r_2(\Pi)(\mathrm{Frob}_v))$ is odd; the existence of such a prime is a consequence of Tchebotarev's density theorem. If we moreover assume that the image is $\mathrm{GL}_2(\mathbb{F}_2)$, a similar trick can be used to find a finite list of primes v for which, if $\mathrm{Tr}(r_2(E)(\mathrm{Frob}_v)) \equiv \mathrm{Tr}(r_2(\Pi)(\mathrm{Frob}_v)) (\mathrm{mod}\, 2)$, then the image of $\overline{\rho_2(\Pi)}$ is also $\mathrm{GL}_2(\mathbb{F}_2)$. At this point we use the Faltings-Serre method (**[Ser85]**) with $\overline{r_2(E)}$ and $\overline{r_2(\Pi)}$, and complete our list of primes on which we have to check equality of traces of Frobenius. The other cases are handled similarly, although the use of the Faltings-Serre method has to be adapted. When the image is not $\mathrm{GL}_2(\mathbb{F}_2)$, we use the following theorem of Livné (**[Liv87]**):

THEOREM. *Let S be a finite set of primes of F, and $L/\mathbb{Q}_2$ a finite extension, with ring of integers $\mathcal{O}_L$ and maximal ideal λ_L. Suppose that $r_1, r_2 : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(L)$ are continuous representations unramified outside S, satisfying:*

(1) $\mathrm{Tr}(r_1) \equiv \mathrm{Tr}(r_2) (\mathrm{mod}\, \lambda_L)$ *and* $\det(r_1) \equiv \det(r_2) (\mathrm{mod}\, \lambda_L)$*;*
(2) there exists a finite set of primes T, disjoint from S, such that
  (i) The image of the set $\{\mathrm{Frob}_v\}_{v \in T}$ *in the* $\mathbb{F}_2$*-vector space* $\mathrm{Gal}(F_S/F)$ *is non-cubic.*
  (ii) $\mathrm{Tr}(r_1(\mathrm{Frob}_v)) = \mathrm{Tr}(r_2(\mathrm{Frob}_v))$ *and* $\det(r_1(\mathrm{Frob}_v)) = \det(r_2(\mathrm{Frob}_v))$ *for all* $v \in T$.

Then r_1 and r_2 have isomorphic semisimplifications.

Here F_S is the compositum of all quadratic extensions of F unramified outside S. The notion of a non-cubic set is not relevant for this introduction, and we refer the reader to Chapter X for the details.

We have also written a few GP routines, available in **[CNT]**, which serve to prove modularity in practical examples. The algorithm takes as input the equation of the field F and the elliptic curve E, and returns in the end a finite list of primes $\{p_1, \ldots, p_m\}$ of $\mathbb{Q}$. In all the cases we treated, m was pretty small, with small prime numbers as well. With that finite list, we compare the traces of Frobenius of E at places dividing the p_i with the Hecke eigenvalues of a modular form. In practical applications of the algorithm, given the elliptic curve, we need to explicitely have a modular form to compare it with. We succeeded to prove modularity for a number of explicit elliptic curves, corresponding to the different cases of residual image, using tables of modular forms calculated Cremona and his school.

Organization

The thesis is divided in two chapters, the first chapter corresponding to modularity lifting theorems, and the second chapter to the algorithmic approach.

Chapter 1: Modularity lifting theorems. Section 1 contains some basic preliminaries. We include some generalities about smooth representations of GL_n of a p-adic field, over $\overline{\mathbb{Q}}_\ell$ or $\overline{\mathbb{F}}_\ell$, which will be used later in the proof of the main theorem. We note that many of the results of this section are also proved in **[CHT08]**, although in a slightly different way. We stress the use of the Bernstein formalism in our proofs; some of them are based on an earlier draft **[HT]** of **[CHT08]**.

In Section 2, we develop the theory of (ℓ-adic) automorphic forms on totally definite unitary groups, and apply the results of Labesse and the construction mentioned above to attach Galois representations to automorphic representations of unitary groups.

In Section 3, we study the Hecke algebras of unitary groups and put everything together to prove the main result of the chapter. More precisely, if $\mathbb{T}$ denotes the (localized) Hecke algebra and R is a certain universal deformation ring of a mod ℓ Galois representation attached to $\mathbb{T}$, we prove that $R^{\mathrm{red}} = \mathbb{T}$. In Section 4, we go back to GL_n and use this result to prove the desired modularity lifting theorems.

Chapter 2: An algorithmic approach. In Section 1, we describe the complete algorithm to determine whether the representations $r_2(E)$ and $r_2(\Pi)$ are isomorphic. In Section 2 we recall the construction of $r_2(\Pi)$ and $r_2(E)$ and their main properties.

Section 3 is devoted to the application of the Faltings-Serre method to our situation, combined with Livne's theorem. In Section 4 we explain the algorithm of Section 1 and include its proof.

In Section 5, we include examples where the algorithm is applied to prove modularity of certain elliptic curves. We include one example of each case, corresponding to the different possible residual images. The GP routines used to calculate these examples are included in Section 6.

Some notation

As a general principle, whenever F is a field and $\overline{F}$ is a chosen separable closure, we write $\Gamma_F = \mathrm{Gal}(\overline{F}/F)$. We also write Γ_F when the choice of $\overline{F}$ is implicit. If F is a number field and v is a place of F, we usually write $\Gamma_v \subset \Gamma_F$ for a decomposition group at v. If v is finite, we denote by q_v the order of the residue field of v.

If L/K is an extension of number fields, $\mathfrak{p} \subset \mathscr{O}_K$ is a prime ideal, and $\mathfrak{q} \subset \mathscr{O}_L$ is a prime ideal above $\mathfrak{p}$, we denote by $e(\mathfrak{q}|\mathfrak{p})$ the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$.

CHAPTER 1

Modularity lifting theorems

Introduction

In this chapter we will prove modularity lifting theorems for Galois representations of any dimension satisfying certain conditions. We largely follow the articles [**CHT08**] and [**Tay08**], where an extra local condition appears. Here we remove that condition, which can be done thanks to the latest developments of the trace formula. We describe with more detail the contents of this chapter.

Section 1 contains some basic preliminaries. We include some generalities about smooth representations of GL_n of a p-adic field, over $\overline{\mathbb{Q}}_\ell$ or $\overline{\mathbb{F}}_\ell$, which will be used later in the proof of the main theorem. We note that many of the results of this section are also proved in [**CHT08**], although in a slightly different way. We stress the use of the Bernstein formalism in our proofs; some of them are based on an earlier draft [**HT**] of [**CHT08**].

In Section 2, we develop the theory of (ℓ-adic) automorphic forms on totally definite unitary groups, and apply the results of Labesse ([**Lab**]) and the constructions of [**CH09, Shi11**] to attach Galois representations to automorphic representations of unitary groups.

In Section 3, we study the Hecke algebras of unitary groups and put everything together to prove the main result of the paper. More precisely, if $\mathbb{T}$ denotes the (localized) Hecke algebra and R is a certain universal deformation ring of a mod ℓ Galois representation attached to $\mathbb{T}$, we prove that $R^{\mathrm{red}} = \mathbb{T}$. In Section 4, we go back to GL_n and use this result to prove the desired modularity lifting theorems. The most general theorem we prove for imaginary CM fields is the following. For the terminology used in the different hypotheses, we refer the reader to the main text.

THEOREM. *Let F^+ be a totally real field, and F a totally imaginary quadratic extension of F^+. Let $n \geqslant 1$ be an integer and $\ell > n$ be a prime number, unramified in F. Let*

$$r : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

be a continuous irreducible representation with the following properties. Let $\overline{r}$ denote the semisimplification of the reduction of r.

(i) $r^c \cong r^\vee(1-n)$.
(ii) *r is unramified at all but finitely many primes.*
(iii) *For every place $v|\ell$ of F, $r|_{\Gamma_v}$ is crystalline.*
(iv) *There is an element $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,\overline{\mathbb{Q}}_\ell)}$ such that*
- *for all $\tau \in \mathrm{Hom}(F^+,\overline{\mathbb{Q}}_\ell)$, we have either*

$$\ell - 1 - n \geqslant a_{\tau,1} \geqslant \cdots \geqslant a_{\tau,n} \geqslant 0$$

or

$$\ell - 1 - n \geqslant a_{\tau c,1} \geqslant \cdots \geqslant a_{\tau c,n} \geqslant 0;$$

- *for all $\tau \in \mathrm{Hom}(F,\overline{\mathbb{Q}}_\ell)$ and every $i = 1,\ldots,n$,*

$$a_{\tau c,i} = -a_{\tau,n+1-i}.$$

- *for all* $\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_\ell)$ *giving rise to a prime* $w|\ell$,
$$\mathrm{HT}_\tau(r|_{\Gamma_w}) = \{j - n - a_{\tau,j}\}_{j=1}^n.$$
In particular, r is Hodge-Tate regular.

(v) $\overline{F}^{\ker(\mathrm{ad}\,\overline{r})}$ *does not contain* $F(\zeta_\ell)$.
(vi) The group $\overline{r}(\mathrm{Gal}(\overline{F}/F(\zeta_\ell)))$ *is big.*
(vii) The representation $\overline{r}$ *is irreducible and there is a conjugate self-dual, cohomological, cuspidal automorphic representation* Π *of* $\mathrm{GL}_n(\mathbb{A}_F)$, *of weight* $\mathbf{a}$ *and unramified above* ℓ, *and an isomorphism* $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$, *such that* $\overline{r} \cong \overline{r}_{\ell,\iota}(\Pi)$.

Then r is automorphic of weight $\mathbf{a}$ *and level prime to* ℓ.

0. Some notation and definitions

0.1. Irreducible algebraic representations of GL_n**.** Let $\mathbb{Z}^{n,+}$ denote the set of n-tuples of integers $a = (a_1, \ldots, a_n)$ such that
$$a_1 \geqslant \cdots \geqslant a_n.$$
Given $a \in \mathbb{Z}^{n,+}$, there is a unique irreducible, finite dimensional, algebraic representation $\xi_a : \mathrm{GL}_n \to \mathrm{GL}(W_a)$ over $\mathbb{Q}$ with highest weight given by
$$\mathrm{diag}(t_1, \ldots, t_n) \mapsto \prod_{i=1}^n t_i^{a_i}.$$
Let E be any field of characteristic zero. Tensoring with E, we obtain an irreducible algebraic representation $W_{a,E}$ of GL_n over E, and every such representation arises in this way. Suppose that $E/\mathbb{Q}$ is a finite extension. Then the irreducible, finite dimensional, algebraic representations of $(\mathrm{Res}_{E/\mathbb{Q}}\,\mathrm{GL}_{n/E})(\mathbb{C})$ are parametrized by elements $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(E,\mathbb{C})}$. We denote them by $(\xi_{\mathbf{a}}, W_{\mathbf{a}})$.

0.2. Local Langlands correspondence. Let p be a rational prime and let F be a finite extension of $\mathbb{Q}_p$. Fix an algebraic closure $\overline{F}$ of F. Fix also a positive integer n, a prime number $\ell \neq p$ and an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$. Let $\mathrm{Art}_F : F^\times \to \Gamma_F^{\mathrm{ab}}$ be the local reciprocity map, normalized to take uniformizers to geometric Frobenius elements. If π is an irreducible smooth representation of $\mathrm{GL}_n(F)$ over $\overline{\mathbb{Q}}_\ell$, we will write $r_\ell(\pi)$ for the ℓ-adic Galois representation associated to the Weil-Deligne representation
$$\mathscr{L}(\pi \otimes |\ |^{(1-n)/2}),$$
where $\mathscr{L}$ denotes the local Langlands correspondence, normalized to coincide with the correspondence induced by Art_F in the case $n = 1$. Note that $r_\ell(\pi)$ does not always exist. The eigenvalues of $\mathscr{L}(\pi \otimes |\ |^{(n-1)/2})(\phi_F)$ must be ℓ-adic units for some lift ϕ_F of the geometric Frobenius (see **[Tat79]**). Whenever we make a statement about $r_\ell(\pi)$, we will suppose that this is the case. Note that our conventions differ from those of **[CHT08]** and **[Tay08]**, where $r_\ell(\pi)$ is defined to be the Galois representation associated to $\mathscr{L}(\pi^\vee \otimes |\ |^{(1-n)/2})$.

0.3. Hodge-Tate weights. Fix a finite extension $L/\mathbb{Q}_\ell$ and an algebraic closure $\overline{L}$ of L. Fix an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$ and an algebraic extension K of $\mathbb{Q}_\ell$ contained in $\overline{\mathbb{Q}}_\ell$ such that K contains every $\mathbb{Q}_\ell$-embedding $L \hookrightarrow \overline{\mathbb{Q}}_\ell$. Suppose that V is a finite dimensional K-vector space equipped with a continuous linear action of Γ_L. Let B_{dR} be the ring of p-adic periods, as in [**Ast94**]. Then $(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_\ell} V)^{\Gamma_L}$ is an $L \otimes_{\mathbb{Q}_\ell} K$-module. We say that V is de Rham if this module is free of rank equal to $\dim_K V$. Since $L \otimes_{\mathbb{Q}_\ell} K \simeq (K)^{\mathrm{Hom}_{\mathbb{Q}_\ell}(L,K)}$, if V is a K-representation of Γ_L, we have that

$$\begin{aligned}(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_\ell} V)^{\Gamma_L} &\simeq \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}_\ell}(L,K)} (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_\ell} V)^{\Gamma_L} \otimes_{L \otimes_{\mathbb{Q}_\ell} K, \tau \otimes 1} K \\ &\simeq \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}_\ell}(L,K)} (B_{\mathrm{dR}} \underset{L,\tau}{\otimes} V)^{\Gamma_L}.\end{aligned}$$

It follows that V is de Rham if and only if

$$\dim_K (B_{\mathrm{dR}} \otimes_{L,\tau} V)^{\Gamma_L} = \dim_K V$$

for every $\tau \in \mathrm{Hom}_{\mathbb{Q}_\ell}(L, K)$. We use the convention of Hodge-Tate weights in which the cyclotomic character has 1 as its unique Hodge-Tate weight. Thus, for V de Rham, we let $\mathrm{HT}_\tau(V)$ be the multiset consisting of the elements $q \in \mathbb{Z}$ such that $\mathrm{gr}^{-q}(B_{\mathrm{dR}} \otimes_{L,\tau} V)^{\Gamma_L} \neq 0$, with multiplicity equal to

$$\dim_K \mathrm{gr}^{-q}(B_{\mathrm{dR}} \otimes_{L,\tau} V)^{\Gamma_L}.$$

Thus, $\mathrm{HT}_\tau(V)$ is a multiset of $\dim_K V$ elements. We say that V is *Hodge-Tate regular* if for every $\tau \in \mathrm{Hom}_{\mathbb{Q}_\ell}(L, K)$, the multiplicity of each Hodge-Tate weight with respect to τ is 1. We make analogous definitions for crystalline representations over K.

0.4. Galois representations of unitary type. Let F be any number field. If ℓ is a prime number, $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$ is an isomorphism and $\psi : \mathbb{A}_F^\times / F^\times \to \mathbb{C}^\times$ is an algebraic character, we denote by $r_{\ell,\iota}(\psi)$ the Galois character associated to it by Lemma 4.1.3 of [**CHT08**].

Let F^+ be a totally real number field, and F/F^+ a totally imaginary quadratic extension. Denote by $c \in \mathrm{Gal}(F/F^+)$ the non-trivial automorphism. Let Π be an irreducible admissible representation of $\mathrm{GL}_n(\mathbb{A}_F)$. We say that Π is *essentially conjugate self dual* if there exists a continuous character $\chi : \mathbb{A}_{F^+}^\times/(F^+)^\times \to \mathbb{C}^\times$ with $\chi_v(-1)$ independent of $v|\infty$ such that

$$\Pi^\vee \cong \Pi^c \otimes (\chi \circ \mathbf{N}_{F/F^+} \circ \det).$$

If we can take $\chi = 1$, that is, if $\Pi^\vee \cong \Pi^c$, we say that Π is *conjugate self dual*.

Let Π be an automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$. We say that Π is *cohomological* if there exists an irreducible, algebraic, finite-dimensional representation W of $\mathrm{Res}_{F/\mathbb{Q}} \mathrm{GL}_n$, such that the infinitesimal character of Π_∞ is the same as that of W. Let $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,\mathbb{C})}$, and let $(\xi_{\mathbf{a}}, W_{\mathbf{a}})$ the irreducible, finite dimensional, algebraic representation of $(\mathrm{Res}_{F/\mathbb{Q}} \mathrm{GL}_n)(\mathbb{C})$ with highest weight $\mathbf{a}$. We say that Π has *weight* $\mathbf{a}$ if it has the same infinitesimal character as $(\xi_{\mathbf{a}}^\vee, W_{\mathbf{a}}^\vee)$.

The next theorem (in the conjugate self dual case) is due to Clozel, Harris and Labesse ([**CHLa, CHLb**]), with some improvements by Chenevier and Harris ([**CH09**]), except that they only provide compatibility of the local and global Langlands correspondences for the unramified places. Shin ([**Shi11**]), using a very slightly different method, obtained the identification at the remaining places. We note that Caraiani ([**Car10**]) proves that the Weil-Deligne representations correspond up to Frobenius semi-simplification, although we do not need this stronger result for our purposes. The slightly more general version of the construction of the Galois representation stated here for an essentially conjugate self dual representation is proved in Theorem 1.2 of [**BLGHT**]. Let $\overline{F}$ be an algebraic closure of F and let $\Gamma_F = \mathrm{Gal}(\overline{F}/F)$. For $m \in \mathbb{Z}$ and $r : \Gamma_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ a continuous representation, we denote by $r(m)$ the m-th Tate twist of r, and by r^{ss} the semisimplification of r. Fix a prime number ℓ, an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$, and an isomorpshim $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$.

THEOREM 0.1. *Let Π be an essentially conjugate self dual, cohomological, cuspidal automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$. More precisely, suppose that $\Pi^\vee \cong \Pi^c \otimes (\chi \circ \mathbf{N}_{F/F^+} \circ \det)$ for some continuous character $\chi : \mathbb{A}_{F^+}^\times/(F^+)^\times \to \mathbb{C}^\times$ with $\chi_v(-1)$ independent of $v|\infty$. Then there exists a continuous semisimple representation*

$$r_\ell(\Pi) = r_{\ell,\iota}(\Pi) : \Gamma_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

with the following properties.

(i) For every finite place $w \nmid \ell$,

$$(r_\ell(\Pi)|_{\Gamma_w})^{\mathrm{ss}} \simeq \left(r_\ell(\iota^{-1}\Pi_w)\right)^{\mathrm{ss}}.$$

(ii) $r_\ell(\Pi)^c \cong r_\ell(\Pi)^\vee(1-n) \otimes r_\ell(\chi^{-1})|_{\Gamma_F}$.

(iii) If $w \nmid \ell$ is a finite place such that Π_w is unramified, then $r_\ell(\Pi)$ is unramified at w.

(iv) For every $w|\ell$, $r_\ell(\Pi)$ is de Rham at w. Moreover, if Π_w is unramified, then $r_\ell(\Pi)$ is crystalline at w.

(v) Suppose that Π has weight $\mathbf{a}$. Then for each $w|\ell$ and each embedding $\tau : F \hookrightarrow \overline{\mathbb{Q}}_\ell$ giving rise to w, the Hodge-Tate weights of $r_\ell(\Pi)|_{\Gamma_w}$ with respect to τ are given by

$$\mathrm{HT}_\tau(r_\ell(\Pi)|_{\Gamma_w}) = \{j - n - a_{\iota\tau,j}\}_{j=1,\ldots,n},$$

and in particular, $r_\ell(\Pi)|_{\Gamma_w}$ is Hodge-Tate regular.

The representation $r_{\ell,\iota}(\Pi)$ can be taken to be valued in the ring of integers of a finite extension of $\mathbb{Q}_\ell$. Thus, we can reduce it modulo its maximal ideal and semisimplify to obtain a well defined continuous semisimple representation

$$\overline{r}_{\ell,\iota}(\Pi) : \Gamma_F \longrightarrow \mathrm{GL}_n(\overline{\mathbb{F}}_\ell).$$

Let $\mathbf{a}$ be an element of $(\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,\overline{\mathbb{Q}}_\ell)}$. Let

$$r : \Gamma_F \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

be a continuous semisimple representation. We say that r is *automorphic of weight* $\mathbf{a}$ if there is an isomorphism $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$ and an essentially conjugate self dual, cohomological, cuspidal automorphic representation Π of $\mathrm{GL}_n(\mathbb{A}_F)$ of weight $\iota_*\mathbf{a}$ such that $r \cong r_{\ell,\iota}(\Pi)$. We say that r is automorphic of weight $\mathbf{a}$ and *level prime to* ℓ if moreover there exists such a pair (ι, Π) with Π_ℓ unramified. Here $\iota_*\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,\mathbb{C})}$ is defined as $(\iota_*\mathbf{a})_\tau = a_{\iota^{-1}\tau}$.

There is an analogous construction for a totally real field F^+. The definition of cohomological is the same, namely, that the infinitesimal character is the same as that of some irreducible algebraic finite dimensional representation of $(\mathrm{Res}_{F^+/\mathbb{Q}}\mathrm{GL}_n)(\mathbb{C})$.

THEOREM 0.2. *Let Π be a cuspidal automorphic representation of $\mathrm{GL}_n(\mathbb{A}_{F^+})$, cohomological of weight $\mathbf{a}$, and suppose that*

$$\Pi^\vee \cong \Pi \otimes (\chi \circ \det),$$

where $\chi : \mathbb{A}_{F^+}^\times/(F^+)^\times \to \mathbb{C}^\times$ is a continuous character such that $\chi_v(-1)$ is independent of $v|\infty$. Let $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$. Then there is a continuous semisimple representation

$$r_\ell(\Pi) = r_{\ell,\iota}(\Pi) : \Gamma_{F^+} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

with the following properties.

(i) *For every finite place $v \nmid \ell$,*

$$(r_\ell(\Pi)|_{\Gamma_v})^{\mathrm{ss}} \simeq \left(r_\ell(\iota^{-1}\Pi_v)\right)^{\mathrm{ss}}.$$

(ii) *$r_\ell(\Pi) \cong r_\ell(\Pi)^\vee(1-n) \otimes r_\ell(\chi^{-1})$.*
(iii) *If $v \nmid \ell$ is a finite place such that Π_v is unramified, then $r_\ell(\Pi)$ is unramified at v.*
(iv) *For every $v|\ell$, $r_\ell(\Pi)$ is de Rham at v. Moreover, if Π_v is unramified, then $r_\ell(\Pi)$ is crystalline at v.*
(v) *For each $v|\ell$ and each embedding $\tau : F^+ \hookrightarrow \overline{\mathbb{Q}}_\ell$ giving rise to v, the Hodge-Tate weights of $r_\ell(\Pi)|_{\Gamma_v}$ with respect to τ are given by*

$$\mathrm{HT}_\tau(r_\ell(\Pi)|_{\Gamma_v}) = \{j - n - a_{\iota\tau,j}\}_{j=1,\ldots,n},$$

and in particular, $r_\ell(\Pi)|_{\Gamma_v}$ is Hodge-Tate regular.

Moreover, if $\psi : \mathbb{A}_{F^+}^\times/(F^+)^\times \to \mathbb{C}^\times$ is an algebraic character, then

$$r_\ell(\Pi \otimes (\psi \circ \det)) = r_\ell(\Pi) \otimes r_\ell(\psi).$$

PROOF. This can be deduced from the last theorem in exactly the same way as Proposition 4.3.1 of **[CHT08]** is deduced from Proposition 4.2.1 of *loc. cit.* □

We analogously define what it means for a Galois representation of a totally real field to be automorphic of some weight $\mathbf{a}$.

0.5. The group scheme $\mathscr{G}_n$. We define (see Chapter 2 of **[CHT08]**) $\mathscr{G}_n$ as the group scheme over $\mathbb{Z}$ given by the semi-direct product of $\mathrm{GL}_n \times \mathrm{GL}_1$ by the group $\{1, j\}$ acting on $\mathrm{GL}_n \times \mathrm{GL}_1$ by

$$j(g, \mu)j^{-1} = (\mu^t g^{-1}, \mu).$$

There is a homomorphism $\nu : \mathscr{G}_n \to \mathrm{GL}_1$ which sends (g, μ) to μ and j to -1. We denote by $\mathscr{G}_n^0$ the connected component of $\mathscr{G}_n$. By $\mathfrak{g}_n$ we denote the Lie algebra of GL_n sitting inside $\mathrm{Lie}\,\mathscr{G}_n$, so that $\mathscr{G}_n$ acts on $\mathfrak{g}_n$ by the adjoint action. We write $\mathfrak{g}_n^0$ for the subspace of $\mathfrak{g}_n$ of elements of trace zero.

If R is any ring, Γ any group, Δ a subgroup of index 2 (in our applications, $\Gamma = \Gamma_F$ and $\Delta = \Gamma_{F^+}$) and $r : \Gamma \to \mathscr{G}_n(R)$ is a homomorphism, we denote by the same letter the homomorphism $r : \Delta \to \mathrm{GL}_n(R)$ obtained by composing the restriction of r to Δ with the natural projection $\mathscr{G}_n(R) \to \mathrm{GL}_n(R)$. We also say that the first homomorphism is an *extension* of the second one.

0.6. Bigness. Let ℓ be a prime number and $k/\mathbb{F}_\ell$ an algebraic extension. We will call a subgroup $H \subset \mathscr{G}_n(k)$ *big* if the following conditions are satisfied.

- $H \cap \mathscr{G}_n^0(k)$ has no ℓ-power order quotient.
- $H^0(H, \mathfrak{g}_n(k)) = 0$.
- $H^1(H, \mathfrak{g}_n(k)) = 0$.
- For all irreducible $k[H]$-submodules W of $\mathfrak{g}_n(k)$, we can find $h \in H \cap \mathscr{G}_n^0(k)$ and $\alpha \in k$ with the following properties. The α-generalized eigenspace $V_{h,\alpha}$ of h in k^n is one dimensional. Let $\pi_{h,\alpha} : k^n \to V_{h,\alpha}$ (resp. $i_{h,\alpha} : V_{h,\alpha} \to k^n$) denote the h-equivariant projection of k^n to $V_{h,\alpha}$ (resp. h-equivariant injection of $V_{h,\alpha}$ into k^n). Then $\pi_{h,\alpha} \circ W \circ i_{h,\alpha} \neq 0$.

Similarly, we call a subgroup $H \subset \mathrm{GL}_n(k)$ *big* if the following conditions are satisfied.

- H has no ℓ-power order quotient.
- $H^0(H, {}_n^0(k)) = 0$.
- $H^1(H, {}_n^0(k)) = 0$.
- For all irreducible $k[H]$-submodules W of $\mathfrak{g}_n^0(k)$, we can find $h \in H \cap \mathscr{G}_n^0(k)$ and $\alpha \in k$ with the following properties. The α-generalized eigenspace $V_{h,\alpha}$ of h in k^n is one dimensional. Let $\pi_{h,\alpha} : k^n \to V_{h,\alpha}$ (resp. $i_{h,\alpha} : V_{h,\alpha} \to k^n$) denote the h-equivariant projection of k^n to $V_{h,\alpha}$ (resp. h-equivariant injection of $V_{h,\alpha}$ into k^n). Then $\pi_{h,\alpha} \circ W \circ i_{h,\alpha} \neq 0$.

See Section 2.5 of **[CHT08]** for several examples of big subgroups.

1. Admissible representations of GL_n of a p-adic field over $\overline{\mathbb{Q}}_\ell$ and $\overline{\mathbb{F}}_\ell$

Let p be a rational prime and let F be a finite extension of $\mathbb{Q}_p$, with ring of integers $\mathscr{O}_F$, maximal ideal λ_F and residue field $k_F = \mathscr{O}_F/\lambda_F$. Let $q = \#k_F$. Let ϖ be a generator of λ_F. We will fix an algebraic closure $\overline{F}$ of F, and write $\Gamma_F = \mathrm{Gal}(\overline{F}/F)$. Corresponding to it, we have an algebraic closure $\overline{k_F}$ of k_F, and we will let Frob_F be the geometric Frobenius in $\mathrm{Gal}(\overline{k_F}/k_F)$ and I_F be the inertia subgroup of Γ_F. Usually we will also write Frob_F for a lift to Γ_F. Fix also a positive integer n, a prime number $\ell \neq p$, an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$ and an algebraic closure $\overline{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$. We will let R be either $\overline{\mathbb{Q}}_\ell$ or $\overline{\mathbb{F}}_\ell$. Denote by $|\,|: F^\times \to q^{\mathbb{Z}} \subset \mathbb{Z}[\frac{1}{q}]$ the absolute value normalized such that $|\varpi| = q^{-1}$. We denote by the same symbol the composition of $|\,|$ and the natural map $\mathbb{Z}[\frac{1}{q}] \to R$, which exists because q is invertible in R. For the general theory of smooth representations over R, we refer the reader to **[Vig96]**. Throughout this section, representation will always mean smooth representation.

For a locally compact, totally disconnected group G, a compact open subgroup $K \subset G$ and an element $g \in G$, we denote by $[KgK]$ the operator in the Hecke algebra of G relative to K corresponding to the (R-valued) characteristic function of the double coset KgK.

Given a tuple $\mathbf{t} = (t^{(1)}, \dots, t^{(n)})$ of elements in any ring A, we denote by $P_{q,\mathbf{t}} \in A[X]$ the polynomial

$$P_{q,\mathbf{t}} = X^n + \sum_{j=1}^{n} (-1)^j q^{j(j-1)/2} t^{(j)} X^{n-j}.$$

We use freely the terms Borel, parabolic, Levi, and so on, to refer to the F-valued points of the corresponding algebraic subgroups of GL_n. Write B for the Borel subgroup of $\mathrm{GL}_n(F)$ consisting of upper triangular matrices, and $B_0 = B \cap \mathrm{GL}_n(\mathcal{O}_F)$. Let $T \simeq (F^\times)^n$ be the standard maximal torus of $\mathrm{GL}_n(F)$. Let N be the group of upper triangular matrices whose diagonal elements are all 1. Then $B = TN$ (semi-direct product). Let $r : \mathrm{GL}_n(\mathcal{O}_F) \to \mathrm{GL}_n(k_F)$ denote the reduction map. We introduce the following subgroups of $\mathrm{GL}_n(\mathcal{O}_F)$:

- $U_0 = \{g \in \mathrm{GL}_n(\mathcal{O}_F) : \ r(g) = \begin{pmatrix} *_{n-1,n-1} & *_{n-1,1} \\ 0_{1,n-1} & * \end{pmatrix}\}$;
- $U_1 = \{g \in \mathrm{GL}_n(\mathcal{O}_F) : \ r(g) = \begin{pmatrix} *_{n-1,n-1} & *_{n-1,1} \\ 0_{1,n-1} & 1 \end{pmatrix}\}$;
- $\mathrm{Iw} = \{g \in \mathrm{GL}_n(\mathcal{O}_F) : \ r(g)$ is upper triangular$\}$;
- $\mathrm{Iw}_1 = \{g \in \mathrm{Iw} : \ r(g)_{ii} = 1 \ \forall i = 1, \dots, n\}$.

Thus, U_1 is a normal subgroup of U_0 and we have a natural identification

$$U_0/U_1 \simeq k_F^\times,$$

and similarly, Iw_1 is a normal subgroup of Iw and we have a natural identification

$$\mathrm{Iw}\,/\,\mathrm{Iw}_1 \simeq (k_F^\times)^n.$$

We denote by $\mathscr{H}$ the R-valued Hecke algebra of $\mathrm{GL}_n(F)$ with respect to $\mathrm{GL}_n(\mathcal{O}_F)$. We do not include R in the notation. For every smooth representation π of $\mathrm{GL}_n(F)$, $\pi^{\mathrm{GL}_n(\mathcal{O}_F)}$ is naturally a left module over $\mathscr{H}$. For $j = 1, \dots, n$, we will let $T_F^{(j)} \in \mathscr{H}$ denote the Hecke operator

$$\left[\mathrm{GL}_n(\mathcal{O}_F) \begin{pmatrix} \varpi 1_j & 0 \\ 0 & 1_{n-j} \end{pmatrix} \mathrm{GL}_n(\mathcal{O}_F)\right].$$

Let π be a representation of $\mathrm{GL}_n(F)$ over $\overline{\mathbb{Q}}_\ell$. We say that π is essentially square-integrable if, under an isomorphism $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$, the corresponding complex representation is essentially square integrable in the usual sense. It is a non trivial fact that the notion of essentially square integrable complex representation is invariant under an automorphism of $\mathbb{C}$, which makes our definition independent of the chosen isomorphism $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$. This can be shown using the Bernstein-Zelevinsky classification of essentially square integrable representations in terms of quotients of parabolic inductions from supercuspidals (see below).

Let $n = n_1 + \cdots + n_r$ be a partition of n and $P \supset B$ the corresponding parabolic subgroup of $\mathrm{GL}_n(F)$. The modular character $\delta_P : P \to \mathbb{Q}^\times$ takes values in $q^{\mathbb{Z}} \subset R^\times$. Choosing once and for all a square root of q in R, we can consider the square root character $\delta_P^{1/2} : P \to R^\times$. For each $i = 1, \dots r$, let π_i be a representation of $\mathrm{GL}_{n_i}(F)$. We denote by $\pi_1 \times \cdots \times \pi_r$ the normalized induction from P to $\mathrm{GL}_n(F)$ of the representation $\pi_1 \otimes \cdots \otimes \pi_r$. Whenever we write $|\,|$ we will mean $|\,| \circ \det$. For any R-valued character β of $F^\times$ and any positive integer m, we denote by $\beta[m]$ the one dimensional representation $\beta \circ \det$ of $\mathrm{GL}_m(F)$.

Suppose that $R = \overline{\mathbb{Q}}_\ell$. Let $n = rk$ and σ be an irreducible supercuspidal representation of $\mathrm{GL}_r(F)$. By a theorem of Bernstein ([**Zel80**, 9.3]),

$$\left(\sigma \otimes |\,|^{\frac{1-k}{2}}\right) \times \cdots \times \left(\sigma \otimes |\,|^{\frac{k-1}{2}}\right)$$

has a unique irreducible quotient denoted $\mathrm{St}_k(\sigma)$, which is essentially square integrable. Moreover, every irreducible, essentially square integrable representation of $\mathrm{GL}_n(F)$ is of the form $\mathrm{St}_k(\sigma)$ for a unique pair (k, σ). Under the local Langlands correspondence $\mathscr{L}$, $\mathrm{St}_k(\sigma)$ corresponds to $\mathrm{Sp}_k \otimes \mathscr{L}(\sigma \otimes |\,|^{\frac{1-k}{2}})$ (see page 252 of [**HT01**] or Section 4.4 of [**Rod82**]), where Sp_k is as in [**Tat79**, 4.1.4]. Suppose now that $n = n_1 + \cdots + n_r$ and that π_i is an irreducible essentially square integrable representation of $\mathrm{GL}_{n_i}(F)$. Then $\pi_1 \times \cdots \times \pi_r$ has a distinguished constituent appearing with multiplicity one, called the Langlands subquotient, which we denote by

$$\pi_1 \boxplus \cdots \boxplus \pi_r.$$

Every irreducible representation of $\mathrm{GL}_n(F)$ over $\overline{\mathbb{Q}}_\ell$ is of this form for some partition of n, and the π_i are well determined modulo permutation ([**Zel80**, 6.1]). The π_i can be ordered in such a way that the Langlands subquotient is actually a quotient of the parabolic induction.

If $\chi_1, \dots, \chi_n$ are unramified characters then

$$\chi_1 \boxplus \cdots \boxplus \chi_n$$

is the unique unramified constituent of $\chi_1 \times \cdots \times \chi_n$, and every irreducible unramified representation of $\mathrm{GL}_n(F)$ over $\overline{\mathbb{Q}}_\ell$ is of this form. Let π be such a representation, corresponding to a $\overline{\mathbb{Q}}_\ell$-algebra morphism $\lambda_\pi : \mathscr{H} \to \overline{\mathbb{Q}}_\ell$. For $j = 1, \dots, n$, let s_j denote the j-th elementary symmetric polynomial in n variables. If we define unramified characters

$$\chi_i : F^\times \to \overline{\mathbb{Q}}_\ell^\times$$

in such a way that $\lambda_\pi(T_F^{(j)}) = q^{j(n-j)/2} s_j(\chi_1(\varpi), \ldots, \chi_n(\varpi))$, then

$$\pi \simeq \chi_1 \boxplus \cdots \boxplus \chi_n.$$

Moreover, by the Iwasawa decomposition $\mathrm{GL}_n(F) = B\,\mathrm{GL}_n(\mathscr{O}_F)$, we have that $\dim_{\overline{\mathbb{Q}}_\ell} \pi^{\mathrm{GL}_n(\mathscr{O}_F)} = 1$. We denote $\mathbf{t}_\pi = (\lambda_\pi(T_F^{(1)}), \ldots, \lambda_\pi(T_F^{(n)}))$.

LEMMA 1.1. *Let π be an irreducible unramified representation of $\mathrm{GL}_n(F)$ over $\overline{\mathbb{Q}}_\ell$. Then the characteristic polynomial of $r_\ell(\pi)(\mathrm{Frob}_F)$ is $P_{q,\mathbf{t}_\pi}$.*

PROOF. Suppose that $\pi = \chi_1 \boxplus \cdots \boxplus \chi_n$. Then

$$r_\ell(\pi) = \bigoplus_{i=1}^{n} (\chi_i \otimes |\,|^{(1-n)/2}) \circ \mathrm{Art}_F^{-1}.$$

Thus, the characteristic polynomial of $r_\ell(\pi)(\mathrm{Frob}_F)$ is

$$\prod_{i=1}^{n}(X - \chi_i(\varpi)q^{(n-1)/2}) = \sum_{j=0}^{n}(-1)^j s_j(\chi_1(\varpi)q^{(n-1)/2}, \ldots, \chi_n(\varpi)q^{(n-1)/2})X^{n-j} = P_{q,\mathbf{t}_\pi}.$$

□

Let $n = n_1 + \cdots + n_r$ be a partition of n and let $\beta_1, \ldots \beta_r$ be *distinct* unramified $\overline{\mathbb{F}}_\ell$-valued characters of $F^\times$. Suppose that $q \equiv 1 (\mathrm{mod}\, \ell)$. Then the representation $\beta_1[n_1] \times \cdots \times \beta_r[n_r]$ is irreducible and unramified, and every irreducible unramified $\overline{\mathbb{F}}_\ell$-representation of $\mathrm{GL}_n(F)$ is obtained in this way. This is proved by Vigneras in [**Vig98**, VI.3]. Moreover, if $\pi = \beta_1[n_1] \times \cdots \times \beta_r[n_r]$, then π is an unramified subrepresentation of the principal series $\beta_1 \times \cdots \times \beta_1 \times \cdots \times \beta_r \times \cdots \times \beta_r$, where β_i appears n_i times. The Iwasawa decomposition implies that the dimension of the $\mathrm{GL}_n(\mathscr{O}_F)$-invariants of this unramified principal series is one, and thus the same is true for π.

A character χ of $F^\times$ is called *tamely ramified* if it is trivial on $1 + \lambda_F$, that is, if its conductor is $\leqslant 1$. In this case, $\chi|_{\mathscr{O}_F^\times}$ has a natural extension to U_0, which we denote by χ^0.

LEMMA 1.2. *Let $\chi_1, \ldots, \chi_n$ be R-valued characters of $F^\times$ such that $\chi_1, \ldots, \chi_{n-1}$ are unramified and χ_n is tamely ramified. Then*

$$\dim_R \mathrm{Hom}_{U_0}(\chi_n^0, \chi_1 \times \cdots \times \chi_n) = \begin{cases} n & \text{if } \chi_n \text{ is unramified} \\ 1 & \text{otherwise.} \end{cases}$$

Furthermore, if χ_n is ramified then $(\chi_1 \times \cdots \times \chi_n)^{U_0} = 0$.

PROOF. Let

$$M(\chi_n^0) = \{f : \mathrm{GL}_n(\mathscr{O}_F) \to R : f(bku) = \chi(b)\chi_n^0(u)f(k)\ \forall\, b \in B_0, k \in \mathrm{GL}_n(\mathscr{O}_F), u \in U_0\},$$

where we write χ for the character of $(F^\times)^n$ given by $\chi_1, \dots, \chi_n$. Then, $\mathrm{Hom}_{U_0}(\chi_n^0, \chi_1 \times \cdots \times \chi_n) = (\chi_1 \times \cdots \times \chi_n)^{U_0 = \chi_n^0}$, which by the Iwasawa decomposition is isomorphic to $M(\chi_n^0)$. By the Bruhat decomposition,

$$B_0 \backslash \mathrm{GL}_n(\mathscr{O}_F)/U_0 \simeq r(B_0)\backslash \mathrm{GL}_n(k_F)/r(U_0) \simeq W_n/W_{n-1},$$

where W_j is the Weyl group of GL_j with respect to its standard maximal split torus. Here we see W_{n-1} inside W_n in the natural way. Let X denote a set of coset representatives of W_n/W_{n-1}, so that

$$\mathrm{GL}_n(\mathscr{O}_F) = \coprod_{w \in X} B_0 w U_0.$$

Thus, if $f \in M(\chi_n^0)$, f is determined by its restriction to the cosets $B_0 w U_0$. We have that

$$M(\chi_n^0) \simeq \prod_{w \in X} M_w,$$

where M_w is the space of functions on $B_0 w U_0$ satisfying the transformation rule of $M(\chi_n^0)$. It is clear that $\dim_R M_w \leqslant 1$ for every w. Moreover, if χ_n is unramified, then M_w is non-zero, a non-zero function being given by $f(w) = 1$. Thus, in this case, $\dim_R M(\chi_n^0) = n$.

In the ramified case, let $a = \mathrm{diag}(a_1, \dots, a_n) \in B_0$, with $a_i \in \mathscr{O}_F^\times$ and a_n such that $\chi_n(a_n) \neq 1$. Then

$$\chi_n(a_n) f(w) = f(aw) = f(wa^w) = \chi_n^0(a^w) f(w) = f(w)$$

unless $w \in W_{n-1}$. Thus, only the identity coset survives, and $\dim_R M(\chi_n^0) = 1$.

For the last assertion, let $f \in (\chi_1 \times \cdots \times \chi_n)$ be U_0-invariant. To see that it is zero, it is enough to see that $f(w) = 0$ for every $w \in X$. Choosing $a \in \mathrm{GL}_n(\mathscr{O}_F)$ to be a scalar matrix corresponding to an element $a \in \mathscr{O}_F^\times$ for which $\chi_n(a) \neq 1$, we see that a is in B_0 (and hence in U_0), thus $f(aw) = \chi_n(a) f(w) = f(wa) = f(w)$, so $f(w) = 0$ for any $w \in X$. $\square$

Let P_M denote the parabolic subgroup of $\mathrm{GL}_n(F)$ containing B corresponding to the partition $n = (n-1) + 1$, and let U_M denote its unipotent radical. Take the Levi decomposition $P_M = MU_M$, where $M \simeq \mathrm{GL}_{n-1}(F) \times \mathrm{GL}_1(F)$. Consider the opposite parabolic subgroup $\overline{P_M}$ with Levi decomposition $\overline{P_M} = M\overline{U_M}$. Let

$$U_{0,M} = U_0 \cap M \simeq \mathrm{GL}_{n-1}(\mathscr{O}_F) \times \mathrm{GL}_1(\mathscr{O}_F).$$

Let χ_n be a tamely ramified character of $F^\times$, and let χ_n^0 be its extension to U_0. Let

$$\mathscr{H}_M(\chi_n) = \mathrm{End}_M(\mathrm{ind}_{U_{0,M}}^M \chi_n),$$

where ind denotes compact induction and χ_n is viewed as a character of $U_{0,M}$ via projection to the last element of the diagonal. Thus, $\mathscr{H}_M(\chi_n)$ can be identified with the R-vector space of compactly supported functions $f : M \to R$ such that $f(kmk') = \chi_n(k)f(m)\chi_n(k')$ for $m \in M$ and $k, k' \in U_{0,M}$. Similarly, let

$$\mathscr{H}_0(\chi_n) = \mathrm{End}_{\mathrm{GL}_n(F)}(\mathrm{ind}_{U_0}^{\mathrm{GL}_n(F)} \chi_n^0).$$

This is identified with the R-vector space of compactly supported functions $f : \mathrm{GL}_n(F) \to R$ such that $f(kgk') = \chi_n^0(k)f(g)\chi_n^0(k')$ for every $g \in \mathrm{GL}_n(F)$, $k, k' \in U_0$. There is a natural injective homomorphism of R-modules

$$\mathscr{T} : \mathscr{H}_M(\chi_n) \to \mathscr{H}_0(\chi_n),$$

which can be described as follows (see **[Vig98**, II.3]). Let $m \in M$. Then $\mathscr{T}(1_{U_{0,M}mU_{0,M}}) = 1_{U_0 m U_0}$, where $1_{U_{0,M}mU_{0,M}}$ is the function supported in $U_{0,M}mU_{0,M}$ whose value at umu' is $\chi_n(u)\chi_n(u')$, and similarly for $1_{U_0 m U_0}$. Define

$$U_0^+ = U_0 \cap U_M$$

and

$$U_0^- = U_0 \cap \overline{U_M}.$$

Then $U_0 = U_0^- U_{0,M} U_0^+ = U_0^+ U_{0,M} U_0^-$, and χ_n^0 is trivial on U_0^- and U_0^+. Let

$$M^- = \{m \in M / \ m^{-1}U_0^+ m \subset U_0^+ \ \text{and} \ mU_0^- m^{-1} \subset U_0^-\}.$$

We denote by $\mathscr{H}_M^-(\chi_n)$ the subspace of $\mathscr{H}_M(\chi_n)$ consisting of functions supported on the union of cosets of the form $U_{0,M}mU_{0,M}$ with $m \in M^-$.

PROPOSITION 1.3. *The subspace $\mathscr{H}_M^-(\chi_n) \subset \mathscr{H}_M(\chi_n)$ is a subalgebra, and the restriction $\mathscr{T}^- : \mathscr{H}_M^-(\chi_n) \to \mathscr{H}_0(\chi_n)$ is an algebra homomorphism.*

PROOF. This is proved in **[Vig98**, II.5]. □

Let π be a representation of $\mathrm{GL}_n(F)$ over R. Then $\mathrm{Hom}_{\mathrm{GL}_n(F)}(\mathrm{ind}_{U_0}^{\mathrm{GL}_n(F)} \chi_n^0, \pi)$ is naturally a right module over $\mathscr{H}_0(\chi_n)$. By the adjointness between compact induction and restriction,

$$\mathrm{Hom}_{\mathrm{GL}_n(F)}(\mathrm{ind}_{U_0}^{\mathrm{GL}_n(F)} \chi_n^0, \pi) = \mathrm{Hom}_{U_0}(\chi_n^0, \pi),$$

and therefore the right hand side is also a right $\mathscr{H}_0(\chi_n)$-module. There is an R-algebra isomorphism $\mathscr{H}_0(\chi_n) \simeq \mathscr{H}_0(\chi_n^{-1})^{\mathrm{opp}}$ given by $f \mapsto f^*$, where $f^*(g) = f(g^{-1})$. We then see $\mathrm{Hom}_{U_0}(\chi_n^0, \pi)$ as a left $\mathscr{H}_0(\chi_n^{-1})$-module in this way. Similarly, $\mathrm{Hom}_{U_{0,M}}(\chi_n, \pi)$ is a left $\mathscr{H}_M(\chi_n^{-1})$-module when π is a representation of M over R. For a representation π of $\mathrm{GL}_n(F)$, let $\pi_{\overline{U_M}}$ be the representation of M obtained by (non-normalized) parabolic restriction. Then the natural projection $\pi \to \pi_{\overline{U_M}}$ is M-linear.

REMARK 1.4. Let $\overline{B_{n-1}}$ denote the subgroup of lower triangular matrices of $\mathrm{GL}_{n-1}(F)$, so that $\overline{B_{n-1}} \times \mathrm{GL}_1(F)$ is a parabolic subgroup of M, with the standard maximal torus $T \subset M$ of $\mathrm{GL}_n(F)$ as a Levi factor. Let $\chi_1, \dots, \chi_n$ be characters of $F^\times$. Then

$$\left((\chi_1 \times \cdots \times \chi_n)_{\overline{U_M}}\right)^{\mathrm{ss}} \simeq \bigoplus_{i=1}^{n} \left(i^M_{B_{n-1}\times \mathrm{GL}_1(F)}(\chi^{w_i})\right)^{\mathrm{ss}} \otimes \delta^{1/2}_{\overline{P_M}}, \tag{1.0.1}$$

where ss denotes semisimplification and $i^M_{B_{n-1}\times \mathrm{GL}_1(F)}$ is the normalized parabolic induction. Here, w_i is the permutation of n letters such that $w_i(n) = n+1-i$ and $w_i(1) > w_i(2) > \cdots > w_i(n-1)$. This follows from Theorem 6.3.5 of **[Cas74]** when $R = \overline{\mathbb{Q}}_\ell$. As Vignéras points out in [**Vig98**, II.2.18], the same proof is valid for the $R = \overline{\mathbb{F}}_\ell$ case.

PROPOSITION 1.5. *Let $\chi_1, \dots, \chi_n$ be R-valued characters of $F^\times$, such that $\chi_1, \dots, \chi_{n-1}$ are unramified and χ_n is tamely ramified.*

(i) The natural projection $\chi_1 \times \cdots \times \chi_n \to (\chi_1 \times \cdots \times \chi_n)_{\overline{U_M}}$ induces an isomorphism of R-modules

$$p : \mathrm{Hom}_{U_0}(\chi_n^0, (\chi_1 \times \cdots \times \chi_n)) \to \mathrm{Hom}_{U_{0,M}}(\chi_n, (\chi_1 \times \cdots \times \chi_n)_{\overline{U_M}}). \tag{1.0.2}$$

(ii) For every $\phi \in \mathrm{Hom}_{U_0}(\chi_n^0, (\chi_1 \cdots \times \dots \chi_n))$ and every $m \in M^-$,

$$p(1_{U_0 m U_0}.\phi) = \delta_{P_M}(m) 1_{U_{0,M} m U_{0,M}}.p(\phi).$$

PROOF. The last assertion is proved in [**Vig98**, II.9]. The fact that p is surjective follows by [**Vig96**, II.3.5]. We prove injectivity now. By Lemma 1.2, the dimension of the left hand side is n if χ_n is unramified and 1 otherwise. Suppose first that $R = \overline{\mathbb{Q}}_\ell$. If χ_n is unramified, each summand of the right hand side of (1.0.1) has a one dimensional $U_{0,M}$-fixed subspace, while if χ_n is ramified, only the summand corresponding to the identity permutation has a one dimensional $U_{0,M}$-fixed subspace, all the rest being zero. This implies that

$$\dim_{\overline{\mathbb{Q}}_\ell}\left((\chi_1 \times \cdots \times \chi_n)_{\overline{U_M}}\right)^{U_{0,M}} = \begin{cases} n & \text{if } \chi_n \text{ is unramified} \\ 1 & \text{otherwise,} \end{cases}$$

Therefore p is an isomorphism for reasons of dimension. This completes the proof of the injectivity of p over $\overline{\mathbb{Q}}_\ell$.

We give the proof over $\overline{\mathbb{F}}_\ell$ only in the unramified case, the ramified case being similar. First of all, note that the result for $\overline{\mathbb{Q}}_\ell$ implies the corresponding result over $\overline{\mathbb{Z}}_\ell$, the ring of integers of $\overline{\mathbb{Q}}_\ell$. Indeed, suppose each χ_i takes values in $\overline{\mathbb{Z}}_\ell^\times$, and let $(\chi_1 \times \cdots \times \chi_n)_{\overline{\mathbb{Z}}_\ell}$ (respectively, $(\chi_1 \times \cdots \times \chi_n)_{\overline{\mathbb{Q}}_\ell}$) denote the parabolic induction over $\overline{\mathbb{Z}}_\ell$ (respectively, $\overline{\mathbb{Q}}_\ell$). Then $(\chi_1 \times \cdots \times \chi_n)_{\overline{\mathbb{Z}}_\ell}$ is a lattice in $(\chi_1 \times \cdots \times \chi_n)_{\overline{\mathbb{Q}}_\ell}$, that is, a free $\overline{\mathbb{Z}}_\ell$-submodule which generates $(\chi_1 \times \cdots \times \chi_n)_{\overline{\mathbb{Q}}_\ell}$ and is $\mathrm{GL}_n(F)$-stable ([**Vig96**, II.4.14(c)]). It then follows that $((\chi_1 \times \cdots \times \chi_n)_{\overline{\mathbb{Z}}_\ell})^{U_0}$ is a lattice in $(\chi_1 \times \cdots \times \chi_n)_{\overline{\mathbb{Q}}_\ell})^{U_0}$ ([**Vig96**, I.9.1]), and so is free of rank n over $\overline{\mathbb{Z}}_\ell$. Simiarly, $((\chi_1 \times \cdots \times \chi_n)_{\overline{U_M},\overline{\mathbb{Z}}_\ell})^{U_{0,M}}$ is a lattice in $((\chi_1 \times \cdots \times \chi_n)_{\overline{U_M},\overline{\mathbb{Q}}_\ell})^{U_{0,M}}$ ([**Vig96**, II.4.14(d)]), and thus it is free of rank n

over $\overline{\mathbb{Z}}_\ell$. Moreover, the map p with coefficients in $\overline{\mathbb{Z}}_\ell$ is still surjective ([**Vig96**, II 3.3]), hence it is an isomorphism by reasons of rank.

Finally, consider the $\overline{\mathbb{F}}_\ell$ case. Choose liftings $\tilde{\chi}_i$ of χ_i to $\overline{\mathbb{Z}}_\ell$-valued characters. Then there is a natural injection

$$(\tilde{\chi}_1 \times \cdots \times \tilde{\chi}_n)_{\overline{U_M}} \otimes_{\overline{\mathbb{Z}}_\ell} \overline{\mathbb{F}}_\ell \hookrightarrow (\chi_1 \times \cdots \times \chi_n)_{\overline{U_M}}$$

inducing an injection

$$((\tilde{\chi}_1 \times \cdots \times \tilde{\chi}_n)_{\overline{U_M}})^{U_{0,M}} \otimes_{\overline{\mathbb{Z}}_\ell} \overline{\mathbb{F}}_\ell \hookrightarrow ((\chi_1 \times \cdots \times \chi_n)_{\overline{U_M}})^{U_{0,M}}. \tag{1.0.3}$$

Now, we have seen that the left hand side of (1.0.3) has dimension n over $\overline{\mathbb{F}}_\ell$. We claim that the right hand side of (1.0.3) has dimension $\leqslant n$. Indeed, by looking at the right hand side of (1.0.1), this follows from the fact that the $U_{0,M}$-invariants of the semisimplification have dimension n. Thus, (1.0.3) is an isomorphism and $\dim_{\overline{\mathbb{F}}_\ell}(\chi_1 \times \cdots \times \chi_n)_{\overline{U_M}})^{U_{0,M}} = n$. Since the left hand side of (1.0.2) has dimension n and p is surjective, it must be an isomorphism. $\square$

Let $\mathscr{H}_0$ (respectively, $\mathscr{H}_1$) be the R-valued Hecke algebra of $\mathrm{GL}_n(F)$ with respect to U_0 (respectively, U_1). Thus, $\mathscr{H}_0 = \mathscr{H}_0(1)$. If π is a representation of $\mathrm{GL}_n(F)$ over R, then π^{U_0} is naturally a left $\mathscr{H}_0$-module. For any $\alpha \in F^\times$ with $|\alpha| \leqslant 1$, let $m_\alpha \in M$ be the element

$$m_\alpha = \begin{pmatrix} 1_{n-1} & 0 \\ 0 & \alpha \end{pmatrix}.$$

For $i = 0$ or 1, let $V_{\alpha,i} \in \mathscr{H}_i$ be the Hecke operators $[U_i m_\alpha U_i]$. If π is a representation of $\mathrm{GL}_n(F)$, then $\pi^{U_0} \subset \pi^{U_1}$ and the action of the operators defined above are compatible with this inclusion.

Let $\mathscr{H}_M = \mathscr{H}_M(1)$, and let $V_{\varpi,M} = [U_{0,M} m_\varpi U_{0,M}] \in \mathscr{H}_M$. Since $m_\varpi \in M^-$, $V_{\varpi,M} \in \mathscr{H}_M^-$, and $\mathscr{T}^-(V_{\varpi,M}) = V_{\varpi,0} \in \mathscr{H}_0$. As above, if π is a representation of M over R, we consider the natural left action $\mathscr{H}_M$ on $\pi^{U_{0,M}}$.

COROLLARY 1.6. *Let $\chi_1, \ldots, \chi_n$ be $\overline{\mathbb{Q}}_\ell$-valued unramified characters of $F^\times$. Then the set of eigenvalues of $V_{\varpi,0}$ acting on the n-dimensional space $(\chi_1 \times \cdots \times \chi_n)^{U_0}$ is equal (counting multiplicities) to $\{q^{(n-1)/2}\chi_i(\varpi)\}_{i=1}^n$.*

PROOF. Note that $V_{\varpi,M}$ acts on the $U_{0,M}$-invariants of each summand of the right hand side of (1.0.1) by the scalar $\chi_i(\varpi)q^{(1-n)/2}$. Thus, the eigenvalues of $V_{\varpi,M}$ in $(\chi_1 \times \cdots \times \chi_n)_{\overline{U_M}}^{U_{0,M}}$ are the $q^{(1-n)/2}\chi_i(\varpi)$. The corollary follows then by Proposition 1.5. $\square$

PROPOSITION 1.7. *Let π be an irreducible unramified representation of* $\mathrm{GL}_n(F)$ *over R. Then $\pi^{U_0} = \pi^{U_1}$ and the following properties hold.*

- *(i) If $R = \overline{\mathbb{Q}}_\ell$ and $\pi = \chi_1 \boxplus \cdots \boxplus \chi_n$, with χ_i unramified characters of $F^\times$, then* $\dim_R \pi^{U_0} \leqslant n$ *and the eigenvalues of $V_{\varpi,0}$ acting on π^{U_0} are contained in $\{q^{(n-1)/2}\chi_i(\varpi)\}_{i=1}^n$ (counting multiplicities).*

(ii) If $R = \overline{\mathbb{F}}_\ell$, $q \equiv 1 (\mathrm{mod}\, \ell)$ and $\pi = \beta_1[n_1] \times \cdots \times \beta_r[n_r]$ with β_i distinct unramified characters of $F^\times$, then $\dim_R \pi^{U_0} = r$ and $V_{\overline{\omega},0}$ acting on π^{U_0} has the r distinct eigenvalues $\{\beta_j(\overline{\omega})\}_{j=1}^r$.

PROOF. The fact that $\pi^{U_1} = \pi^{U_0}$ follows immediately because the central character of π is unramified. Since taking U_0-invariants is exact in characteristic zero, part (i) is clear from the last corollary. Let us prove (ii). Let P be the parabolic subgroup of $\mathrm{GL}_n(F)$ containing B corresponding to the partition $n = n_1 + \cdots + n_r$. As usual, since $\mathrm{GL}_n(F) = P\,\mathrm{GL}_n(\mathscr{O}_F)$, the $\overline{\mathbb{F}}_\ell$-dimension of π^{U_0} is equal to the cardinality of $(\mathrm{GL}_n(\mathscr{O}_F) \cap P) \backslash \mathrm{GL}_n(\mathscr{O}_F)/U_0$. By the Bruhat decomposition, this equals the cardinality of

$$\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_r} \backslash \mathfrak{S}_n / \mathfrak{S}_{n-1} \times \mathfrak{S}_1,$$

where $\mathfrak{S}_i$ is the symmetric group on i letters. This cardinality is easily seen to be r.

It remains to prove the assertion about the eigenvalues of $V_{\overline{\omega},0}$ on π^{U_0}. Let us first replace U_0 by Iw (this was first suggested by Vignéras). By the Iwasawa decomposition and the Bruhat decomposition,

$$\mathrm{GL}_n(F) = \coprod_{s \in S} Ps\,\mathrm{Iw},$$

where $S \subset \mathrm{GL}_n(F)$ is a set of representatives for $(\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_r}) \backslash \mathfrak{S}_n$. Then π^{Iw} has as a basis the set $\{\varphi_s\}_{s \in S}$, where φ_s is supported on $Ps\,\mathrm{Iw}$ and $\varphi_s(s) = 1$.

Let $\mathscr{H}_{\overline{\mathbb{F}}_\ell}(n,1)$ denote the Iwahori-Hecke algebra for $\mathrm{GL}_n(F)$ over $\overline{\mathbb{F}}_\ell$, that is, the Hecke algebra for $\mathrm{GL}_n(F)$ with respect to the compact open subgroup Iw. Thus, π^{Iw} is naturally a left module over $\mathscr{H}_{\overline{\mathbb{F}}_\ell}(n,1)$. For $i = 1, \ldots, n-1$, let s_i denote the n by n permutation matrix corresponding to the transposition $(i\ i+1)$, and let $S_i = [\mathrm{Iw}\, s_i\, \mathrm{Iw}] \in \mathscr{H}_{\overline{\mathbb{F}}_\ell}(n,1)$. For $j = 0, \ldots, n$, let t_j denote the diagonal matrix whose first j coordinates are equal to $\overline{\omega}$, and whose last $n-j$ coordinates are equal to 1. Let $T_j = [\mathrm{Iw}\, t_j\, \mathrm{Iw}] \in \mathscr{H}_{\overline{\mathbb{F}}_\ell}(n,1)$, and for $j = 1, \ldots, n$, let $X_j = T_j(T_{j-1}^{-1})$. Then $\mathscr{H}_{\overline{\mathbb{F}}_\ell}(n,1)$ is generated as an $\overline{\mathbb{F}}_\ell$-algebra by $\{S_i\}_{i=1}^{n-1} \cup \{X_1, X_1^{-1}\}$ ([**Vig96**, I.3.14]). We denote by $\mathscr{H}^0_{\overline{\mathbb{F}}_\ell}(n,1)$ the subalgebra generated by $\{S_i\}_{i=1}^{n-1}$, which is canonically isomorphic to the group algebra $\overline{\mathbb{F}}_\ell[\mathfrak{S}_n]$ of the symmetric group ([**Vig96**, I.3.12]). It can also be identified with the Hecke algebra of $\mathrm{GL}_n(\mathscr{O}_F)$ with respect to Iw ([**Vig96**, I.3.14]). The subalgebra $A = \overline{\mathbb{F}}_\ell[\{X_i^{\pm}\}_{i=1}^n]$ is commutative, and characters of T can be seen as characters on A. Let $\chi_1, \ldots, \chi_n : F^\times \to \overline{\mathbb{F}}_\ell^\times$ be the characters defined by

$$\chi_1 = \cdots = \chi_{n_1} = \beta_1;$$
$$\cdots;$$
$$\chi_{n_1+\cdots+n_{j-1}+1} = \cdots = \chi_{n_1+\cdots+n_j} = \beta_j;$$
$$\cdots.$$

Then the action of A on φ_s is given by the character $s(\chi)$. Note that the set $\{s(\chi)\}_{s \in S}$ is just the set of n-tuples of characters in which β_i occurs n_i times, with arbitrary order. It is clear that for each $j = 1, \dots, r$, there is at least one $s \in S$ for which $s(n) \in \{n_1 + \dots + n_{j-1} + 1, \dots, n_1 + \dots + n_j\}$, so that $X_n \varphi_s = \beta_j(\overline{\omega})\varphi_s$. Let

$$\varphi = \sum_{s \in S} \varphi_s.$$

Then φ generates $\pi^{\mathrm{GL}_n(\mathscr{O}_F)}$. For $j = 1, \dots, r$, let

$$\psi_j = \sum_{s \in S, \chi_{s(n)} = \beta_j} \varphi_s.$$

We have seen above that $\psi_j \neq 0$. Moreover, $X_n \psi_j = \beta_j(\overline{\omega})\psi_j$. Let $P_j \in \overline{\mathbb{F}}_\ell[X]$ be a polynomial such that $P_j(\beta_j(\overline{\omega})) = 1$ and $P_j(\beta_i(\overline{\omega})) = 0$ for every $i \neq j$. Then $\psi_j = P_j(X_n)\varphi$, and it follows that the r distinct eigenvalues $\{\beta_j(\overline{\omega})\}_{j=1}^r$ of X_n on π^{Iw} already occur on the subspace $\overline{\mathbb{F}}_\ell[X_n]\varphi$.

Consider now the map $p_T : \pi^{\mathrm{Iw}} \to (\pi_{\overline{N}})^{T_0}$, where $\overline{N}$ is the unipotent radical of the parabolic subgroup of $\mathrm{GL}_n(F)$ containing T, opposite to B, and $T_0 = T \cap \mathrm{GL}_n(\mathscr{O}_F)$. By [**Vig96**, II.3.5], p_T is an isomorphism. On the other hand, there is a commutative diagram

$$\begin{array}{ccc} \pi^{U_0} & \xrightarrow{\ i\ } & \pi^{\mathrm{Iw}} \\ {\scriptstyle p_M}\downarrow & & \downarrow{\scriptstyle p_T} \\ (\pi_{\overline{U_M}})^{U_{0,M}} & \xrightarrow{p_{M,T}} & (\pi_{\overline{N}})^{T_0}, \end{array}$$

where i is the inclusion and p_M and $p_{M,T}$ are the natural projection to the coinvariants. The analogues of part (ii) of Proposition 1.5 for p_M, p_T and $p_{M,T}$ are still valid ([**Vig98**, II.9]). Thus, for $f \in \pi^{U_0}$,

$$\begin{aligned} p_T(i(V_{\overline{\omega},0}f)) &= p_{M,T}(p_M(V_{\overline{\omega},0}f)) = p_{M,T}([U_{0,M}m_{\overline{\omega}}U_{0,M}]p_M(f)) = \\ &= [T_0 m_{\overline{\omega}} T_0]p_{M,T}(p_M(f)) = [T_0 m_{\overline{\omega}} T_0]p_T(i(f)) = p_T(X_n i(f)). \end{aligned}$$

It follows that $V_{\overline{\omega},0} = X_n$ on π^{U_0}. In particular, $\overline{\mathbb{F}}_\ell[X_n]\varphi = \overline{\mathbb{F}}_\ell[V_{\overline{\omega},0}]\varphi \subset \pi^{U_0}$. By what we have seen above, we conclude that the eigenvalues of $V_{\overline{\omega},0}$ on the r dimensional space π^{U_0} are $\{\beta_j(\overline{\omega})\}_{j=1}^r$, as claimed. $\square$

COROLLARY 1.8. *Suppose that $q \equiv 1 (\mathrm{mod}\, \ell)$ and let π be an irreducible unramified representation of $\mathrm{GL}_n(F)$ over $\overline{\mathbb{F}}_\ell$. Let $\varphi \in \pi^{\mathrm{GL}_n(\mathscr{O}_F)}$ be a non-zero spherical vector. Then φ generates π^{U_0} as a module over the algebra $\overline{\mathbb{F}}_\ell[V_{\overline{\omega},0}]$.*

PROOF. This is actually a corollary of the proof of the above proposition. Indeed, $V_{\overline{\omega},0}$ has r distinct eigenvalues on $\overline{\mathbb{F}}_\ell[V_{\overline{\omega},0}]\varphi \subset \pi^{U_0}$, and $\dim_{\overline{\mathbb{F}}_\ell} \pi^{U_0} = r$. $\square$

LEMMA 1.9. *Let π be an irreducible representation of $\mathrm{GL}_n(F)$ over $\overline{\mathbb{Q}}_\ell$ with a non-zero U_1-fixed vector but no non-zero $\mathrm{GL}_n(\mathscr{O}_F)$-fixed vectors. Then $\dim_{\overline{\mathbb{Q}}_\ell} \pi^{U_1} = 1$ and there is a character*

$$V_\pi : F^\times \to \overline{\mathbb{Q}}_\ell^\times$$

with open kernel such that for every $\alpha \in F^\times$ with non-negative valuation, $V_\pi(\alpha)$ is the eigenvalue of $V_{\alpha,1}$ on π^{U_1}. Moreover, there is an exact sequence

$$0 \longrightarrow s \longrightarrow r_\ell(\pi) \longrightarrow V_\pi \circ \mathrm{Art}_F^{-1} \longrightarrow 0,$$

where s is unramified. If $\pi^{U_0} \neq 0$ then $q^{-1}V_\pi(\overline{\omega})$ is a root of the characteristic polynomial of $s(\mathrm{Frob}_F)$. If, on the other hand, if $\pi^{U_0} = 0$, then $r_\ell(\pi)(\mathrm{Gal}(\overline{F}/F))$ is abelian.

PROOF. This is Lemma 3.1.5 of **[CHT08]**. The proof basically consists in noting that if $\pi^{U_1} \neq 0$, then either $\pi \simeq \chi_1 \boxplus \cdots \boxplus \chi_n$ with $\chi_1, \ldots, \chi_{n-1}$ unramified and χ_n tamely ramified, or $\pi \simeq \chi_1 \boxplus \cdots \boxplus \chi_{n-2} \boxplus \mathrm{St}_2(\chi_{n-1})$ with $\chi_1, \ldots, \chi_{n-1}$ unramified. Then one just analyzes the cases separately, and calculates explicitly the action of the operators $U_{F,1}^{(j)}$ (see **[CHT08]** for their definition) and $V_{\alpha,1}$. $\square$

LEMMA 1.10. *Suppose that $q \equiv 1 (\mathrm{mod}\ \ell)$, and let π be an irreducible unramified representation of $\mathrm{GL}_n(F)$ over $\overline{\mathbb{F}}_\ell$. Let $\lambda_\pi(T_F^{(j)})$ be the eigenvalue of $T_F^{(j)}$ on $\pi^{\mathrm{GL}_n(\mathscr{O}_F)}$, and $\mathbf{t}_\pi = (\lambda_\pi(T_F^{(1)}), \ldots, \lambda_\pi(T_F^{(n)}))$. Suppose that $P_{q,\mathbf{t}_\pi} = (X-a)^m F(X)$ in $\overline{\mathbb{F}}_\ell[X]$, with $m > 0$ and $F(a) \neq 0$. Then $F(V_{\overline{\omega},0})$, as an operator acting on π^{U_0}, is non-zero on the subspace $\pi^{\mathrm{GL}_n(\mathscr{O}_F)}$.*

PROOF. Suppose on the contrary that $F(V_{\overline{\omega},0})(\pi^{\mathrm{GL}_n(\mathscr{O}_F)}) = 0$. Let $\varphi \in \pi^{\mathrm{GL}_n(\mathscr{O}_F)}$ be a non-zero element. Suppose that $\pi = \beta_1[n_1] \times \cdots \times \beta_r[n_r]$, with β_i distinct unramified $\overline{\mathbb{F}}_\ell^\times$-valued characters of $F^\times$. Then, since $q = 1$ in $\overline{\mathbb{F}}_\ell$,

$$P_{q,\mathbf{t}_\pi} = \prod_{i=1}^{r} (X - \beta_i(\overline{\omega}))^{n_i}.$$

Suppose that $a = \beta_j(\overline{\omega}_1)$, so that $F(X) = \prod_{i \neq j}(X - \beta_i(\overline{\omega}))^{n_i}$. By Proposition 1.7 (ii), π^{U_0} has dimension r and $V_{\overline{\omega},0}$ is diagonalizable on this space, with distinct eigenvalues $\beta_i(\overline{\omega})$. Let $\varphi_j \in \pi^{U_0}$ denote an eigenfunction of $V_{\overline{\omega},0}$ of eigenvalue $\beta_j(\overline{\omega})$. By Corollary 1.8, there exists a polynomial $P_j \in \overline{\mathbb{F}}_\ell[X]$ such that $\varphi_j = P_j(V_{\overline{\omega},0})(\varphi)$. Since polynomials in $V_{\overline{\omega},0}$ commute with each other, we must have $F(V_{\overline{\omega},0})(\varphi_j) = 0$, but this also equals $F(\beta_j(\overline{\omega}))\varphi_j \neq 0$, which is a contradiction. $\square$

2. Automorphic forms on unitary groups

2.1. Totally definite groups. Let F^+ be a totally real field and F a totally imaginary quadratic extension of F^+. Denote by $c \in \mathrm{Gal}(F/F^+)$ the non-trivial Galois automorphism. Let $n \geqslant 1$ be an integer and V an n-dimensional vector space over F, equipped with a non-degenerate c-hermitian form $h : V \times V \to F$. To the pair (V, h) there is attached a reductive algebraic group $U(V,h)$ over F^+, whose points in an F^+-algebra R are

$$U(V,h)(R) = \{g \in \mathrm{Aut}_{(F \otimes_{F^+} R)-\mathrm{lin}}(V \otimes_{F^+} R) : h(gx, gy) = h(x,y)\ \forall x, y \in V \otimes_{F^+} R\}.$$

By an *unitary group* attached to F/F^+ in n variables, we shall mean an algebraic group of the form $U(V,h)$ for some pair (V,h) as above. Let G be such a group. Then $G_F = G \otimes_{F^+} F$ is isomorphic to GL_V, and in fact it is an outer form of GL_V. Let $G(F^+_\infty) = \prod_{v|\infty} G(F^+_v)$, and if v is any place of F^+, let $G_v = G \otimes_{F^+} F^+_v$. We say that G is *totally definite* if $G(F^+_\infty)$ is compact (and thus isomorphic to a product of copies of the compact unitary group $U(n)$).

Suppose that v is a place of F^+ which splits in F, and let w be a place of F above v, corresponding to an F^+-embedding $\sigma_w : F \hookrightarrow \overline{F^+_v}$. Then $F^+_v = \sigma_w(F)F^+_v$ is an F-algebra by means of σ_w, and thus G_v is isomorphic to $\mathrm{GL}_{V\otimes F^+_v}$, the tensor product being over F. Note that if we choose another place w^c of F above v, then σ_w and σ_{w^c} give F^+_v two different F-algebra structures. If we choose a basis of V, we obtain two isomorphisms $i_w, i_{w^c} : G_v \to \mathrm{GL}_{n/F^+_v}$. If $X \in \mathrm{GL}_n(F)$ is the matrix of h in the chosen basis, then for any F^+_v-algebra R and any $g \in G_v(R)$, $i_{w^c}(g) = X^{-1}({}^t i_w(g)^{-1})X$, where we see $X \in \mathrm{GL}_n(R)$ via $\sigma_w : F \to F^+_v \to R$.

The choice of a lattice L in V such that $h(L \times L) \subset \mathscr{O}_F$ gives an affine group scheme over $\mathscr{O}_{F^+}$, still denoted by G, which is isomorphic to G after extending scalars to F^+. We will fix from now on a basis for L over $\mathscr{O}_F$, giving also an F-basis for V; with respect to these, for each split place v of F^+ and each place w of F above v, i_w gives an isomorphism between $G(F^+_v)$ and $\mathrm{GL}_n(F_w)$ taking $G(\mathscr{O}_{F^+_v})$ to $\mathrm{GL}_n(\mathscr{O}_{F_w})$.

2.2. Automorphic forms. Let G be a totally definite unitary group in n variables attached to F/F^+. We let $\mathscr{A}$ denote the space of automorphic forms on $G(\mathbb{A}_{F^+})$. Since the group is totally definite, $\mathscr{A}$ decomposes, as a representation of $G(\mathbb{A}_{F^+})$, as

$$\mathscr{A} \cong \bigoplus_{\pi} m(\pi)\pi,$$

where π runs through the isomorphism classes of irreducible admissible representations of $G(\mathbb{A}_{F^+})$, and $m(\pi)$ is the multiplicity of π in $\mathscr{A}$, which is always finite. This is a well known fact for any reductive group compact at infinity, but we recall the proof as a warm up for the following sections and to set some notation. The isomorphism classes of continuous, complex, irreducible (and hence finite dimensional) representations of $G(F^+_\infty)$ are parametrized by elements $\mathbf{b} = (b_\tau) \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F^+,\mathbb{R})}$. We denote them by $W_\mathbf{b}$. Since $G(F^+_\infty)$ is compact and every element of $\mathscr{A}$ is $G(F^+_\infty)$-finite, $\mathscr{A}$ decomposes as a direct sum of irreducible $G(\mathbb{A}_{F^+})$-submodules. Moreover, we can write

$$\mathscr{A} \cong \bigoplus_{\mathbf{b}} W_\mathbf{b} \otimes \mathrm{Hom}_{G(F^+_\infty)}(W_\mathbf{b}, \mathscr{A})$$

as $G(\mathbb{A}_{F^+})$-modules. Denote by $\mathbb{A}^\infty_{F^+}$ the ring of finite adèles. For any $\mathbf{b}$, let $S_\mathbf{b}$ be the space of smooth (that is, locally constant) functions $f : G(\mathbb{A}^\infty_{F^+}) \to W^\vee_\mathbf{b}$ such that $f(\gamma g) = \gamma_\infty f(g)$ for all $g \in G(\mathbb{A}^\infty_{F^+})$ and $\gamma \in G(F^+)$. Then the map

$$f \mapsto \Big(w \mapsto \Big(g \mapsto (g_\infty^{-1} f(g^\infty))(w)\Big)\Big)$$

induces a $G(\mathbb{A}_{F^+}^\infty)$-isomorphism between $\mathrm{Hom}_{G(F_\infty^+)}(W_{\mathbf{b}}, \mathscr{A})$ and $S_{\mathbf{b}}$, where the action on this last space is by right translation. For every compact open subgroup $U \subset G(\mathbb{A}_{F^+}^\infty)$, the space $G(F)\backslash G(\mathbb{A}_{F^+}^\infty)/U$ is finite, and hence the space of U-invariants of $S_{\mathbf{b}}$ is finite-dimensional. In particular, every irreducible summand of $W_{\mathbf{b}} \otimes \mathrm{Hom}_{G(F_\infty^+)}(W_{\mathbf{b}}, \mathscr{A})$ is admissible and appears with finite multiplicity. Thus, every irreducible summand of $\mathscr{A}$ is admissible, and appears with finite multiplicity because its isotypic component is contained in $W_{\mathbf{b}} \otimes \mathrm{Hom}_{G(F_\infty^+)}(W_{\mathbf{b}}, \mathscr{A})$ for some $\mathbf{b}$.

2.3. ℓ-adic models of automorphic forms. Let ℓ be an odd prime number. We will assume, from now on to the end of this section, that every place of F^+ above ℓ splits in F. Let K be a finite extension of $\mathbb{Q}_\ell$. Fix an algebraic closure $\overline{K}$ of K, and suppose that K is big enough to contain all embeddings of F into $\overline{K}$. Let $\mathscr{O}$ be its ring of integers and λ its maximal ideal. Let S_ℓ denote the set of places of F^+ above ℓ, and I_ℓ the set of embeddings $F^+ \hookrightarrow K$. Thus, there is a natural surjection $h : I_\ell \twoheadrightarrow S_\ell$. Let $\widetilde{S}_\ell$ denote a set of places of F such that $\widetilde{S}_\ell \coprod \widetilde{S}_\ell^c$ consists of all the places above S_ℓ; thus, there is a bijection $S_\ell \simeq \widetilde{S}_\ell$. For $v \in S_\ell$, we denote by $\tilde{v}$ the corresponding place in $\widetilde{S}_\ell$. Also, let $\widetilde{I}_\ell$ denote the set of embeddings $F \hookrightarrow K$ giving rise to a place in $\widetilde{S}_\ell$. Thus, there is a bijection between I_ℓ and $\widetilde{I}_\ell$, which we denote by $\tau \mapsto \tilde{\tau}$. Also, denote by $\tau \mapsto w_\tau$ the natural surjection $\widetilde{I}_\ell \to \widetilde{S}_\ell$. Finally, Let $F_\ell^+ = \prod_{v|\ell} F_v^+$.

Let $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,K)}$. Consider the following representation of $G(F_\ell^+) \simeq \prod_{\tilde{v}\in\widetilde{S}_\ell} \mathrm{GL}_n(F_{\tilde{v}})$. For each $\tilde{\tau} \in \widetilde{I}_\ell$, we have an embedding $\mathrm{GL}_n(F_{w_{\tilde{\tau}}}) \hookrightarrow \mathrm{GL}_n(K)$. Taking the product over $\tilde{\tau}$ and composing with the projection on the $w_{\tilde{\tau}}$-coordinates, we have an irreducible representation

$$\xi_{\mathbf{a}} : G(F_\ell^+) \longrightarrow \mathrm{GL}(W_{\mathbf{a}}),$$

where $W_{\mathbf{a}} = \otimes_{\tilde{\tau}\in\widetilde{I}_\ell} W_{a_{\tilde{\tau}},K}$. This representation has an integral model $\xi_{\mathbf{a}} : G(\mathscr{O}_{F_\ell^+}) \to \mathrm{GL}(M_{\mathbf{a}})$. In order to base change to automorphic representations of GL_n, we need to impose the additional assumption that

$$a_{\tau c,i} = -a_{\tau,n+1-i}$$

for every $\tau \in \mathrm{Hom}(F, K)$ and every $i = 1, \ldots, n$.

Besides the weight, we will have to introduce another collection of data, away from ℓ, for defining our automorphic forms. This will take care of the level-raising arguments needed later on. Let S_r be a finite set of places of F^+, split in F and disjoint from S_ℓ. For $v \in S_r$, let $U_{0,v} \subset G(F_v^+)$ be a compact open subgroup, and let

$$\chi_v : U_{0,v} \to \mathscr{O}^\times$$

be a morphism with open kernel. We will use the notation $U_r = \prod_{v\in S_r} U_{0,v}$ and $\chi = \prod_{v\in S_r} \chi_v$.

Fix the data $\{\mathbf{a}, U_r, \chi\}$. Let $M_{\mathbf{a},\chi} = M_{\mathbf{a}} \otimes_{\mathscr{O}} (\bigotimes_{v\in S_r} \mathscr{O}(\chi_v))$. Let $U \subset G(\mathbb{A}_{F^+}^\infty)$ be a compact open subgroup such that its projection to the v-th coordinate is contained in $U_{0,v}$ for each $v \in S_r$. Let A be an $\mathscr{O}$-algebra. Suppose either that the projection of U to

$G(F_\ell^+)$ is contained in $G(\mathcal{O}_{F_\ell^+})$, or that A is a K-algebra. Then define $S_{\mathbf{a},\chi}(U,A)$ to be the space of functions

$$f : G(F^+)\backslash G(\mathbb{A}_{F^+}^\infty) \to M_{\mathbf{a},\chi} \otimes_{\mathcal{O}} A$$

such that

$$f(gu) = u_{\ell,S_r}^{-1} f(g) \quad \forall\, g \in G(\mathbb{A}_{F^+}^\infty), u \in U,$$

where u_{ℓ,S_r} denotes the product of the projections to the coordinates of S_ℓ and S_r. Here, u_{S_r} acts already on $M_{\mathbf{a},\chi}$ by χ, and the action of u_ℓ is via $\xi_{\mathbf{a}}$.

Let V be any compact subgroup of $G(\mathbb{A}_{F^+}^\infty)$ such that its projection to $G(F_v^+)$ is contained in $U_{0,v}$ for each $v \in S_r$, and let A be an $\mathcal{O}$-algebra. If either A is a K-algebra or the projection of V to $G(F_\ell^+)$ is contained in $G(\mathcal{O}_{F_\ell^+})$, denote by $S_{\mathbf{a},\chi}(V,A)$ the union of the $S_{\mathbf{a},\chi}(U,A)$, where U runs over compact open subgroups containing V for which their projection to $G(F_v^+)$ is contained in $U_{0,v}$ for each $v \in S_r$, and for which their projection to $G(F_\ell^+)$ is contained in $G(\mathcal{O}_{F_\ell^+})$ if A is not a K-algebra. Note that if $V \subset V'$ then $S_{\mathbf{a},\chi}(V',A) \subset S_{\mathbf{a},\chi}(V,A)$.

If U is open and we choose a decomposition

$$G(\mathbb{A}_{F^+}^\infty) = \coprod_{j\in J} G(F^+) g_j U,$$

then the map $f \mapsto (f(g_j))_{j\in J}$ defines an injection of A-modules

$$S_{\mathbf{a},\chi}(U,A) \hookrightarrow \prod_{j\in J} M_{\mathbf{a},\chi} \otimes_{\mathcal{O}} A. \tag{2.3.1}$$

Since $G(F^+)\backslash G(\mathbb{A}_{F^+}^\infty)/U$ is finite and $M_{\mathbf{a},\chi}$ is a free $\mathcal{O}$-module of finite rank, we have that $S_{\mathbf{a},\chi}(U,A)$ is a finitely generated A-module.

We say that a compact open subgroup $U \subset G(\mathbb{A}_{F^+}^\infty)$ is sufficiently small if for some finite place v of F^+, the projection of U to $G(F_v^+)$ contains only one element of finite order. Note that the map (2.3.1) is not always surjective, but it is if, for example, U is sufficiently small. Thus, in this case, $S_{\mathbf{a},\chi}(U,A)$ is a free A-module of rank

$$(\dim_K W_{\mathbf{a}}).\#\left(G(F^+)\backslash G(\mathbb{A}_{F^+}^\infty)/U\right).$$

Moreover, if either U is sufficiently small or A is $\mathcal{O}$-flat, we have that

$$S_{\mathbf{a},\chi}(U,A) = S_{\mathbf{a},\chi}(U,\mathcal{O}) \otimes_{\mathcal{O}} A.$$

Let U and V be compact subgroups of $G(\mathbb{A}_{F^+}^\infty)$ such that their projections to $G(F_v^+)$ are contained in $U_{0,v}$ for each $v \in S_r$. Suppose either A is a K-algebra or that the projections of U and V to $G(F_\ell^+)$ are contained in $G(\mathcal{O}_{F_\ell^+})$. Also, let $g \in G(\mathbb{A}_{F^+}^{S_r,\infty}) \times U_r$; if A is not a K-algebra, we suppose that $g_\ell \in G(\mathcal{O}_{F_\ell^+})$. If $V \subset gUg^{-1}$, then there is a natural map

$$g : S_{\mathbf{a},\chi}(U,A) \longrightarrow S_{\mathbf{a},\chi}(V,A)$$

defined by

$$(gf)(h) = g_{\ell,S_r} f(hg).$$

In particular, if V is a normal subgroup of U, then U acts on $S_{\mathbf{a},\chi}(V,A)$, and we have that

$$S_{\mathbf{a},\chi}(U,A) = S_{\mathbf{a},\chi}(V,A)^U.$$

Let U_1 and U_2 be compact subgroups of $G(\mathbb{A}^{\infty}_{F^+})$ such that their projections to $G(F^+_v)$ are contained in $U_{0,v}$ for all $v \in S_r$. Let $g \in G(\mathbb{A}^{S_r,\infty}_{F^+}) \times U_r$. If A is not a K-algebra, we suppose that the projections of U_1 and U_2 to $G(F^+_\ell)$ are contained in $G(\mathcal{O}_{F^+_\ell})$, and that $g_\ell \in G(\mathcal{O}_{F^+_\ell})$. Suppose also that $\# U_1 g U_2/U_2 < \infty$ (this will be automatic if U_1 and U_2 are open). Then we can define an A-linear map

$$[U_1 g U_2] : S_{\mathbf{a},\chi}(U_2,A) \longrightarrow S_{\mathbf{a},\chi}(U_1,A)$$

by

$$([U_1 g U_2] f)(h) = \sum_i (g_i)_{\ell,S_r} f(h g_i),$$

if $U_1 g U_2 = \coprod_i g_i U_2$.

LEMMA 2.1. *Let $U \subset G(\mathbb{A}^{\infty,S_r}_{F^+}) \times \prod_{v\in S_r} U_{0,v}$ be a sufficiently small compact open subgroup and let $V \subset U$ be a normal open subgroup. Let A be an $\mathcal{O}$-algebra. Suppose that either A is a K-algebra or the projection of U to $G(F^+_\ell)$ is contained in $G(\mathcal{O}_{F^+_\ell})$. Then $S_{\mathbf{a},\chi}(V,A)$ is a finite free $A[U/V]$-module. Moreover, let $I_{U/V} \subset A[U/V]$ be the augmentation ideal and let $S_{\mathbf{a},\chi}(V,A)_{U/V} = S_{\mathbf{a},\chi}(V,A)/I_{U/V} S_{\mathbf{a},\chi}(V,A)$ be the module of coinvariants. Define*

$$\mathrm{Tr}_{U/V} : S_{\mathbf{a},\chi}(V,A)_{U/V} \to S_{\mathbf{a},\chi}(U,A) = S_{\mathbf{a},\chi}(V,A)^U$$

as $\mathrm{Tr}_{U/V}(f) = \sum_{u\in U/V} uf$. Then $\mathrm{Tr}_{U/V}$ is an isomorphism.

PROOF. This is the analog of Lemma 3.3.1 of **[CHT08]**, and can be proved in the same way. □

Choose an isomorphism $\iota : \overline{K} \xrightarrow{\simeq} \mathbb{C}$. The choice of $\widetilde{I}_\ell$ gives a bijection

$$\iota^+_* : (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,K)}_c \xrightarrow{\sim} (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F^+,\mathbb{R})}, \tag{2.3.2}$$

where $(\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,K)}_c$ denotes the set of elements $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,K)}$ such that

$$a_{\tau c,i} = -a_{\tau,n+1-i}$$

for every $\tau \in \mathrm{Hom}(F,K)$ and every $i = 1,\dots,n$. The map is given by $(\iota^+_* \mathbf{a})_\tau = a_{\widetilde{\iota^{-1}\tau}}$. We have an isomorphism $\theta : W_{\mathbf{a}} \otimes_{K,\iota} \mathbb{C} \to W_{\iota^+_* \mathbf{a}}$. Then the map

$$S_{\mathbf{a},\emptyset}(\{1\},\mathbb{C}) \longrightarrow S_{(\iota^+_*\mathbf{a})^\vee}$$

given by

$$f \mapsto (g \mapsto \theta(g_\ell f(g)))$$

is an isomorphism of $\mathbb{C}[G(\mathbb{A}^\infty_{F^+})]$-modules, where, $(\iota^+_*\mathbf{a})^\vee_{\tau,i} = -(\iota^+_*\mathbf{a})_{\tau,n+1-i}$. Its inverse is given by

$$\phi \mapsto (g \mapsto g_\ell^{-1}\theta^{-1}(\phi(g))).$$

It follows that $S_{\mathbf{a},\varnothing}(\{1\},\mathbb{C})$ is a semi-simple admissible module. Hence, $S_{\mathbf{a},\varnothing}(\{1\},\overline{K})$ is also semi-simple admissible, and this easily implies that $S_{\mathbf{a},\chi}(U_r,\overline{K})$ is a semi-simple admissible $G(\mathbb{A}_{F^+}^{\infty,S_r})$-module. If $\pi \subset S_{\mathbf{a},\varnothing}(\{1\},\overline{K})$ is an irreducible $G(\mathbb{A}_{F^+}^{\infty,S_r}) \times U_r$-constituent such that the subspace on which U_r acts by χ^{-1} is non-zero, then this subspace is an irreducible constituent of $S_{\mathbf{a},\chi}(U_r,\overline{K})$, and every irreducible constituent of it is obtained in this way.

2.4. Base change and descent. Keep the notation as above. We will assume from now on the following hypotheses.

- F/F^+ is unramified at all finite places.
- G_v is quasi-split for every finite place v.

It is not a very serious restriction for the applications we have in mind, because we will always be able to base change to this situation. First, note that given F/F^+, if n is odd there always exists a totally definite unitary group G in n variables with G_v quasi-split for every finite v. If n is even, such a G exists if and only if $[F^+ : \mathbb{Q}]n/2$ is also even. This follows from the general classification of unitary groups over number fields in terms of the local Hasse invariants.

Let $G_n^* = \mathrm{Res}_{F/F^+}(\mathrm{GL}_n)$. Let v be a finite place of F^+, so that G_v is an unramified group. In particular, it contains hyperspecial maximal compact subgroups. Let σ_v be any irreducible admissible representation of $G(F_v^+)$. If v is split in F, or if v is inert and σ_v is spherical, there exists an irreducible admissible representation $\mathrm{BC}_v(\sigma_v)$ of $G_n^*(F_v^+)$, called the *local base change* of σ_v, with the following properties. Suppose that v is inert and σ_v is a spherical representation of $G(F_v^+)$; then $\mathrm{BC}_v(\sigma_v)$ is an unramified representation of $G_n^*(F_v^+)$, whose Satake parameters are explicitly determined in terms of those of σ_v; the formula is given in [**Min**], where we take the *standard base change* defined there. If v splits in F as ww^c, the local base change in this case is $\mathrm{BC}_v(\sigma_v) = \sigma_v \circ i_w^{-1} \otimes (\sigma_v \circ i_{w^c}^{-1})^\vee$ as a representation of $G_n^*(F_v^+) = \mathrm{GL}_n(F_w) \times \mathrm{GL}_n(F_{w^c})$. In this way, if we see $\mathrm{BC}_v(\sigma_v)$ as a representation of $G(F_v^+) \times G(F_v^+)$ via the isomorphism $i_w \times i_{w^c} : G(F_v^+) \times G(F_v^+) \xrightarrow{\sim} \mathrm{GL}_n(F_w) \times \mathrm{GL}_n(F_{w^c})$, then $\mathrm{BC}_v(\sigma_v) = \sigma_v \otimes \sigma_v^\vee$. The base change for ramified finite places is being treated in the work of Mœglin, but for our applications it is enough to assume that F/F^+ is unramified at finite places.

In the global case, if σ is an automorphic representation of $G(\mathbb{A}_{F^+})$, we say that an automorphic representation Π of $G_n^*(\mathbb{A}_{F^+}) = \mathrm{GL}_n(\mathbb{A}_F)$ is a (strong) base change of σ if Π_v is the local base change of σ_v for every finite v, except those inert v where σ_v is not spherical, and if the infinitesimal character of Π_∞ is the base change of that of σ_∞. In particular, since $G(F_\infty^+)$ is compact, Π is cohomological.

The following theorem is one of the main results of [**Lab**], and a key ingredient in this paper. We use the notation $\boxplus$ for the isobaric sum of discrete automorphic representations, as in [**Clo90**].

THEOREM 2.2 (Labesse). *Let σ be an automorphic representation of $G(\mathbb{A}_{F^+})$. Then there exists a partition*

$$n = n_1 + \cdots + n_r$$

and discrete, conjugate self dual automorphic representations Π_i *of* $\mathrm{GL}_{n_i}(\mathbb{A}_F)$*, for* $i = 1, \ldots, r$*, such that*

$$\Pi_1 \boxplus \cdots \boxplus \Pi_r$$

is a base change of σ*.*

Conversely, let Π *be a conjugate self dual, cuspidal, cohomological automorphic representation of* $\mathrm{GL}_n(\mathbb{A}_F)$*. Then* Π *is the base change of an automorphic representation* σ *of* $G(\mathbb{A}_{F^+})$*. Moreover, if such a* σ *satisfies that* σ_v *is spherical for every inert place* v *of* F^+*, then* σ *appears with multiplicity one in the cuspidal spectrum of* G*.*

PROOF. The first part is Corollaire 5.3 of **[Lab]** and the second is Théorème 5.4. □

REMARKS. (1) In **[Lab]** there are two hypothesis to Corollaire 5.3, namely, the property called (*) by Labesse and that σ_∞ is a discrete series, which are automatically satisfied in our case because the group is totally definite.

(2) Since $\Pi_1 \boxplus \cdots \boxplus \Pi_r$ is a base change of σ, it is a cohomological representation of $\mathrm{GL}_n(\mathbb{A}_F)$. However, this doesn't imply that each Π_i is cohomological, although it will be if $n - n_i$ is even.

(3) The partition $n = n_1 + \cdots n_r$ and the representations Π_i are uniquely determined by multiplicity one for GL_n, because the Π_i are discrete.

2.5. Galois representations of unitary type via unitary groups. Keep the notation and assumptions as in the last sections.

THEOREM 2.3. *Let* π *be as above. Let* $\pi = \otimes_{v \notin S_r} \pi_v$ *be an irreducible constituent of the space* $S_{\mathbf{a},\chi}(U_r, \overline{K})$*. Then there exists a unique continuous semisimple representation*

$$r_\ell(\pi) : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{K})$$

satisfying the following properties.

(i) If $v \notin S_\ell \cup S_r$ *is a place of* F^+ *which splits as* $v = ww^c$ *in* F*, then*

$$r_\ell(\pi)|_{\Gamma_w}^{\mathrm{ss}} \simeq \left(r_\ell(\pi_v \circ i_w^{-1})\right)^{\mathrm{ss}}.$$

(ii) $r_\ell(\pi)^c \cong r_\ell(\pi)^\vee(1-n)$*.*

(iii) If v *is an inert place such that* π_v *is spherical then* $r_\ell(\pi)$ *is unramified at* v*.*

(iv) If $w|\ell$ *then* $r_\ell(\pi)$ *is de Rham at* w*, and if moreover* $\pi_{w|_{F^+}}$ *is unramified, then* $r_\ell(\pi)$ *is crystalline at* w*.*

(v) For every $\tau \in \mathrm{Hom}(F, K)$ *giving rise to an place* $w|\ell$ *of* F*, the Hodge-Tate weights of* $r|_{\Gamma_w}$ *with respect to* τ *are given by*

$$\mathrm{HT}_\tau(r|_{\Gamma_w}) = \{j - n - a_{\tau,j}\}_{j=1,\ldots,n}.$$

In particular, r *is Hodge-Tate regular.*

PROOF. For the uniqueness, note that the set of places w of F which are split over a place v of F^+ which is not in $S_\ell \cup S_r$ has Dirichlet density 1, and hence, if two continuous semisimple representations $\mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ satisfy property (i), they are isomorphic.

Take an isomorphism $\iota : \overline{K} \xrightarrow{\sim} \mathbb{C}$. By the above argument, the representation we will construct will not depend on it. By means of ι and the choice of $\widetilde{I}_\ell$, we obtain a (necessarily cuspidal) automorphic representation $\sigma = \otimes_v \sigma_v$ of $G(\mathbb{A}_{F^+})$, such that $\sigma_v = \iota\pi_v$ for $v \notin S_r$ finite and σ_∞ is the representation of $G(F^+_\infty)$ given by the weight $(\iota^+_* \mathbf{a})^\vee \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F^+,\mathbb{R})}$. By Theorem 2.2, there is a partition $n = n_1 + \cdots + n_r$ and discrete automorphic representations Π_i of $\mathrm{GL}_{n_i}(\mathbb{A}_F)$ such that

$$\Pi = \Pi_1 \boxplus \cdots \boxplus \Pi_r$$

is a strong base change of σ. Moreover, Π is cohomological of weight $\iota_* \mathbf{a}$, where $(\iota_* \mathbf{a})_\tau = \mathbf{a}_{\iota^{-1}\tau}$ for $\tau \in \mathrm{Hom}(F,\mathbb{C})$. For each $i = 1, \ldots, r$, let $S_i \supset S_\ell$ be any finite set of finite primes of F^+, unramified in F. For each $i = 1, \ldots, r$, let $\psi_i : \mathbb{A}_F^\times / F^\times \to \mathbb{C}^\times$ be a character such that

- $\psi_i^{-1} = \psi_i^c$;
- ψ_i is unramified above S_i, and
- for every $\tau \in \mathrm{Hom}(F,\mathbb{C})$ giving rise to an infinite place w, we have
$$\psi_{i,w}(z) = (\tau z / |\tau z|)^{\delta_{i,\tau}},$$
where $|z|^2 = z\overline{z}$ and $\delta_{i,\tau} = 0$ if $n - n_i$ is even, and $\delta_{i,\tau} = \pm 1$ otherwise.

Thus, if $n - n_i$ is even, we may just choose $\psi_i = 1$. The proof of the existence of such a character follows from a similar argument used in the proof of [**HT01**, Lemma VII.2.8]. With these choices, it follows that $\Pi_i \psi_i$ is cohomological. Also, by the classification of Mœglin and Waldspurger ([**MW89**]), there is a factorization $n_i = a_i b_i$, and a cuspidal automorphic representation ρ_i of $\mathrm{GL}_{a_i}(\mathbb{A}_F)$ such that

$$\Pi_i \psi_i = \rho_i \boxplus \rho_i |\ | \boxplus \cdots \boxplus \rho_i |\ |^{b_i - 1}.$$

Moreover, $\rho_i |\ |^{\frac{b_i-1}{2}}$ is cuspidal and conjugate self dual. Let $\chi_i : \mathbb{A}_F^\times / F^\times \to \mathbb{C}^\times$ be a character such that

- $\chi_i^{-1} = \chi_i^c$;
- χ_i is unramified above S_i, and
- for every $\tau \in \mathrm{Hom}(F,\mathbb{C})$ giving rise to an infinite place w, we have
$$\chi_{i,w}(z) = (\tau z / |\tau z|)^{\mu_{i,\tau}},$$
where $\mu_{i,\tau} = 0$ if a_i is odd or b_i is odd, and $\mu_{i,\tau} = \pm 1$ otherwise.

Then $\rho_i |\ |^{\frac{b_i-1}{2}} \chi_i$ is cuspidal, cohomological and conjugate self dual. Note that $\chi_i^{-1} |\ |^{(a_i-1)(b_i-1)/2}$ and $\psi_i^{-1} |\ |^{\frac{n_i-n}{2}}$ are algebraic characters. Let

$$\begin{aligned} r_\ell(\pi) = \ & \bigoplus_{i=1}^r \left(r_\ell \left(\rho_i \chi_i |\ |^{\frac{b_i-1}{2}} \right) \otimes \epsilon^{a_i - n_i} \otimes r_\ell \left(\chi_i^{-1} |\ |^{(a_i-1)(b_i-1)/2} \right) \right. \\ & \left. \otimes \left(1 \oplus \epsilon \oplus \cdots \oplus \epsilon^{b_i-1}\right) \otimes r_\ell \left(\psi_i^{-1} |\ |^{\frac{n_i-n}{2}} \right) \right), \end{aligned}$$

where $r_\ell = r_{\ell,\iota}$ and ϵ is the ℓ-adic cyclotomic character. This is a continuous semisimple representation which satisfies all the required properties. We use the freedom to vary the sets S_i to achieve property (iii). $\square$

REMARK 2.4. In the proof of the above theorem, if $r = 1$ and Π is already cuspidal, then $r_\ell(\pi) \cong r_{\ell,\iota}(\Pi)$. As a consequence, suppose that $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$ is an isomorphism and Π is a conjugate self dual, cohomological, cuspidal automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$ of weight $\iota_* \mathbf{a}$. Then, by Theorem 2.2, we can find an irreducible constituent $\pi \subset S_{\mathbf{a},\varnothing}(\{1\}, \overline{K})$ such that $r_{\ell,\iota}(\Pi) \cong r_\ell(\pi)$.

REMARK 2.5. If $r_\ell(\pi)$ is irreducible, then the base change of π is already cuspidal. Indeed, from the construction made in the proof and Remark 2.4, (2), we see that $r_\ell(\pi)$ is a direct sum of r representations r_i of dimension n_i. If $r_\ell(\pi)$ is irreducible, we must have $r = 1$. Similarly, the discrete base change Π must be cuspidal, because otherwise there would be a factorization $n = ab$ with $a, b > 1$ and $r_\ell(\pi)$ would be a direct sum of b representations of dimension a. This proves our claim.

3. An $R^{\mathrm{red}} = T$ theorem for Hecke algebras of unitary groups

3.1. Hecke algebras. Keep the notation and assumptions as in the last section. For each place w of F, split above a place v of F^+, let $\mathrm{Iw}(w) \subset G(\mathcal{O}_{F_v^+})$ be the inverse image under i_w of the group of matrices in $\mathrm{GL}_n(\mathcal{O}_{F_w})$ which reduce modulo w to an upper triangular matrix. Let $\mathrm{Iw}_1(w)$ be the kernel of the natural surjection $\mathrm{Iw}(w) \to (k_w^\times)^n$, where k_w is the residue field of F_w. Similarly, let $U_0(w)$ (resp. $U_1(w)$) be the inverse image under i_w of the group of matrices in $\mathrm{GL}_n(\mathcal{O}_{F_w})$ whose reduction modulo w has last row $(0, \ldots, 0, *)$ (resp. $(0, \ldots, 0, 1)$). Then $U_1(w)$ is a normal subgroup of $U_0(w)$, and the quotient $U_0(w)/U_1(w)$ is naturally isomorphic to $k_w^\times$.

Let Q be a finite (possibly empty) set of places of F^+ split in F, disjoint from S_ℓ and S_r, and let $T \supset S_r \cup S_\ell \cup Q$ be a finite set of places of F^+ split in F. Let $\widetilde{T}$ denote a set of primes of F above T such that $\widetilde{T} \coprod \widetilde{T}^c$ is the set of all primes of F above T. For $v \in T$, we denote by $\widetilde{v}$ the corresponding element of $\widetilde{T}$, and for $S \subset T$, we denote by $\widetilde{S}$ the set of places of F consisting of the $\widetilde{v}$ for $v \in T$. Let

$$U = \prod_v U_v \subset G(\mathbb{A}_{F^+}^\infty)$$

be a sufficiently small compact open subgroup such that:

- if $v \notin T$ splits in F then $U_v = G(\mathcal{O}_{F_v^+})$;
- if $v \in S_r$ then $U_v = \mathrm{Iw}(\widetilde{v})$;
- if $v \in Q$ then $U_v = U_1(\widetilde{v})$;
- if $v \in S_\ell$ then $U_v \subset G(\mathcal{O}_{F_v^+})$.

We write $U_r = \prod_{v \in S_r} U_v$. For $v \in S_r$, let χ_v be an $\mathcal{O}$-valued character of $\mathrm{Iw}(\widetilde{v})$, trivial on $\mathrm{Iw}_1(\widetilde{v})$. Since $\mathrm{Iw}(\widetilde{v}) / \mathrm{Iw}_1(\widetilde{v}) \simeq (k_{\widetilde{v}}^\times)^n$, χ_v is of the form

$$g \mapsto \prod_{i=1}^n \chi_{v,i}(g_{ii}),$$

where $\chi_{v,i} : k_{\widetilde{v}}^\times \to \mathcal{O}^\times$.

Let w be a place of F, split over a place v of F^+ which is not in T. We translate the Hecke operators $T_{F_w}^{(j)}$ for $j = 1, \ldots, n$ on $\mathrm{GL}_n(\mathcal{O}_{F_w})$ to G via the isomorphism i_w. More precisely, let $g_w^{(j)}$ denote the element of $G(\mathbb{A}_{F^+}^{\infty})$ whose v-coordinate is

$$i_w^{-1} \begin{pmatrix} \varpi_w 1_j & 0 \\ 0 & 1_{n-j} \end{pmatrix},$$

and with all other coordinates equal to 1. Then we define $T_w^{(j)}$ to be the operator $[U g_w^{(j)} U]$ of $S_{\mathbf{a},\chi}(U, A)$. We will denote by $\mathbb{T}_{\mathbf{a},\chi}^T(U)$ the $\mathcal{O}$-subalgebra of $\mathrm{End}_{\mathcal{O}}(S_{\mathbf{a},\chi}(U, \mathcal{O}))$ generated by the operators $T_w^{(j)}$ for $j = 1, \ldots, n$ and $(T_w^{(n)})^{-1}$, where w runs over places of F which are split over a place of F^+ not in T. The algebra $\mathbb{T}_{\mathbf{a},\chi}^T(U)$ is reduced, and finite free as an $\mathcal{O}$-module (see **[CHT08]**). Since $\mathcal{O}$ is a domain, this also implies that $\mathbb{T}_{\mathbf{a},\chi}^T(U)$ is a semi-local ring. If $v \in Q$, we can also translate the Hecke operators $V_{\alpha,1}$ of Section 1, for $\alpha \in F_{\tilde{v}}^{\times}$ with non-negative valuation, in exactly the same manner to operators in $S_{\mathbf{a},\chi}(U, A)$, and similarly for $V_{\alpha,0}$ if $U_v = U_0(\tilde{v})$.

Write

$$S_{\mathbf{a},\chi}(U, \overline{K}) = \oplus_{\pi} \pi^U, \qquad (3.1.1)$$

where π runs over the irreducible constituents of $S_{\mathbf{a},\chi}(U_r, \overline{K})$ for which $\pi^U \neq 0$. The Hecke algebra $\mathbb{T}_{\mathbf{a},\chi}^T(U)$ acts on each π^U by a scalar, say, by

$$\lambda_\pi : \mathbb{T}_{\mathbf{a},\chi}^T(U) \longrightarrow \overline{K}.$$

Then, $\ker(\lambda_\pi)$ is a minimal prime ideal of $\mathbb{T}_{\mathbf{a},\chi}^T(U)$, and every minimal prime is of this form. If $\mathfrak{m} \subset \mathbb{T}_{\mathbf{a},\chi}^T(U)$ is a maximal ideal, then

$$S_{\mathbf{a},\chi}(U, \overline{K})_{\mathfrak{m}} \neq 0,$$

and localizing at $\mathfrak{m}$ kills all the representations π such that $\ker(\lambda_\pi) \not\subset \mathfrak{m}$. Note also that $\mathbb{T}_{\mathbf{a},\chi}^T(U)/\mathfrak{m}$ is a finite extension of k. For w a place of F, split over a place $v \notin T$, we will denote by $\mathbf{T}_w$ the n-tuple $(T_w^{(1)}, \ldots, T_w^{(n)})$ of elements of $\mathbb{T}_{\mathbf{a},\chi}^T(U)$. We denote by $\overline{\mathbf{T}}_w$ its reduction modulo $\mathfrak{m}$. We use the notation of section 2.4.1 of **[CHT08]** regarding torsion crystalline representations and Fontaine-Laffaille modules.

PROPOSITION 3.1. *Suppose that $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}_{\mathbf{a},\chi}^T(U)$ with residue field k. Then there is a unique continuous semisimple representation*

$$\bar{r}_{\mathfrak{m}} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(k)$$

with the following properties. The first two already characterize $\bar{r}_{\mathfrak{m}}$ uniquely.

(i) $\bar{r}_{\mathfrak{m}}$ is unramified at all but finitely many places.
(ii) If a place $v \notin T$ splits as ww^c in F then $\bar{r}_{\mathfrak{m}}$ is unramified at w and $\bar{r}_{\mathfrak{m}}(\mathrm{Frob}_w)$ has characteristic polynomial $P_{q_w,\overline{\mathbf{T}}_w}(X)$.
(iii) $\bar{r}_{\mathfrak{m}}^c \cong \bar{r}_{\mathfrak{m}}^{\vee}(1-n)$.

(iv) *If a place v of F^+ is inert in F and if U_v is a hyperspecial maximal compact subgroup of $G(F_v^+)$, then $\overline{r}_{\mathfrak{m}}$ is unramified above v.*

(v) *If $w \in \widetilde{S}_\ell$ is unramified over ℓ, $U_{w|_{F^+}} = G(\mathscr{O}_{F_w^+})$ and for every $\tau \in \widetilde{I}_\ell$ above w we have that*

$$\ell - 1 - n \geqslant a_{\tau,1} \geqslant \cdots \geqslant a_{\tau,n} \geqslant 0,$$

then

$$\overline{r}_{\mathfrak{m}}|_{\Gamma_w} = \mathbf{G}_w(\overline{M}_{\mathfrak{m},w})$$

for some object $\overline{M}_{\mathfrak{m},w}$ of $\mathscr{MF}_{k,w}$. Moreover, for every $\tau \in \widetilde{I}_\ell$ over w, we have

$$\dim_k(\mathrm{gr}^{-i}\,\overline{M}_{\mathfrak{m},w}) \otimes_{\mathscr{O}_{F_w} \otimes_{\mathbb{Z}_\ell} \mathscr{O}, \tau\otimes 1} \mathscr{O} = 1$$

if $i = j - n - a_{\tau,j}$ for some $j = 1, \ldots, n$, and 0 otherwise.

PROOF. Choose a minimal prime ideal $\mathfrak{p} \subset \mathfrak{m}$ and an irreducible constituent π of

$$S_{\mathbf{a},\chi}(U_r, \overline{K})$$

such that $\pi^U \neq 0$ and $\mathbb{T}^T_{\mathbf{a},\chi}(U)$ acts on π^U via $\mathbb{T}^T_{\mathbf{a},\chi}(U)/\mathfrak{p}$. Choose an invariant lattice for $r_\ell(\pi)$ and define then $\overline{r}_{\mathfrak{m}}$ to be the semi-simplification of the reduction of $r_\ell(\pi)$. This satisfies all of the statements of the proposition, except for the fact that a priori it takes values on the algebraic closure of k. Since all the characteristic polynomials of the elements on the image of $\overline{r}_{\mathfrak{m}}$ have coefficients in k, we may assume (because k is finite) that, after conjugation, $\overline{r}_{\mathfrak{m}}$ actually takes values in k. □

We say that a maximal ideal $\mathfrak{m} \subset \mathbb{T}^T_{a,\chi}(U)$ is *Eisenstein* if $\overline{r}_{\mathfrak{m}}$ is absolutely reducible. Recall the definition of the group scheme $\mathscr{G}_n$ given in 0.5.

PROPOSITION 3.2. *Let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of $\mathbb{T}^T_{a,\chi}(U)$, with residue field equal to k. Then $\overline{r}_{\mathfrak{m}}$ has an extension to a continuous morphism*

$$\overline{r}_{\mathfrak{m}} : \mathrm{Gal}(\overline{F}/F^+) \to \mathscr{G}_n(k).$$

Pick such an extension. Then there is a unique continuous lifting

$$r_{\mathfrak{m}} : \mathrm{Gal}(\overline{F}/F^+) \to \mathscr{G}_n(\mathbb{T}^T_{a,\chi}(U)_{\mathfrak{m}})$$

of $\overline{r}_{\mathfrak{m}}$ with the following properties. The first two of these already characterize the lifting $r_{\mathfrak{m}}$ uniquely.

(i) *$r_{\mathfrak{m}}$ is unramified at almost all places.*

(ii) *If a place $v \notin T$ of F^+ splits as ww^c in F, then $r_{\mathfrak{m}}$ is unramified at w and $r_{\mathfrak{m}}(\mathrm{Frob}_w)$ has characteristic polynomial $P_{q_w,\mathbf{T}_w}(X)$.*

(iii) *$\nu \circ r_{\mathfrak{m}} = \epsilon^{1-n}\delta_{F/F^+}^{\mu_{\mathfrak{m}}}$, where δ_{F/F^+} is the non-trivial character of $\mathrm{Gal}(F/F^+)$ and $\mu_{\mathfrak{m}} \in \mathbb{Z}/2\mathbb{Z}$.*

(iv) *If v is an inert place of F^+ such that U_v is a hyperspecial maximal compact subgroup of $G(F_v^+)$ then $r_{\mathfrak{m}}$ is unramified at v.*

(v) *Suppose that $w \in \widetilde{S}_\ell$ is unramified over ℓ, that $U_{w|_{F^+}} = G(\mathcal{O}_{F^+_w})$, and that for every $\tau \in \widetilde{I}_\ell$ above w we have that*
$$\ell - 1 - n \geqslant a_{\tau,1} \geqslant \cdots \geqslant a_{\tau,n} \geqslant 0.$$
Then for each open ideal $I \subset \mathbb{T}^T_{\mathbf{a},\chi}(U)_{\mathfrak{m}}$,
$$\left(r_{\mathfrak{m}} \otimes_{\mathbb{T}^T_{\mathbf{a},\chi}(U)_{\mathfrak{m}}} \mathbb{T}^T_{\mathbf{a},\chi}(U)_{\mathfrak{m}}/I\right)|_{\Gamma_w} = \mathbf{G}_w(M_{\mathfrak{m},I,w})$$
for some object $M_{\mathfrak{m},I,w}$ of $\mathcal{MF}_{\mathcal{O},w}$.

(vi) *If $v \in S_r$ and $\sigma \in I_{F_{\widetilde{v}}}$ then $r_{\mathfrak{m}}(\sigma)$ has characteristic polynomial*
$$\prod_{j=1}^{n}(X - \chi_{v,j}^{-1}(\mathrm{Art}_{F_{\widetilde{v}}}^{-1}\sigma)).$$

(vii) *Suppose that $v \in Q$. Let $\phi_{\widetilde{v}}$ be a lift of $\mathrm{Frob}_{\widetilde{v}}$ to $\mathrm{Gal}(\overline{F}_{\widetilde{v}}/F_{\widetilde{v}})$. Suppose that $\alpha \in k$ is a simple root of the characteristic polynomial of $\overline{r}_{\mathfrak{m}}(\phi_{\widetilde{v}})$. Then there exists a unique root $\widetilde{\alpha} \in \mathbb{T}^T_{\mathbf{a},\chi}(U)_{\mathfrak{m}}$ of the characteristic polynomial of $r_{\mathfrak{m}}(\phi_{\widetilde{v}})$ which lifts α.*

Let $\varpi_{\widetilde{v}}$ be the uniformizer of $F_{\widetilde{v}}$ corresponding to $\phi_{\widetilde{v}}$ via $\mathrm{Art}_{F_{\widetilde{v}}}$. Suppose that $Y \subset S_{\mathbf{a},\chi}(U,K)_{\mathfrak{m}}$ is a $\mathbb{T}^T_{\mathbf{a},\chi}(U)[V_{\varpi_{\widetilde{v}},1}]$-invariant subspace such that $V_{\varpi_{\widetilde{v}},1} - \widetilde{\alpha}$ is topologically nilpotent on Y, and let $\mathbb{T}^T(Y)$ denote the image of $\mathbb{T}^T_{\mathbf{a},\chi}(U)$ in $\mathrm{End}_K(Y)$. Then for each $\beta \in F_{\widetilde{v}}^\times$ with non-negative valuation, $V_{\beta,1}$ (in $\mathrm{End}_K(Y)$) lies in $\mathbb{T}^T(Y)$, and $\beta \mapsto V(\beta)$ extends to a continuous character $V : F_{\widetilde{v}}^\times \to \mathbb{T}^T(Y)^\times$. Further, $(X - V_{\varpi_{\widetilde{v}},1})$ divides the characteristic polynomial of $r_{\mathfrak{m}}(\phi_{\widetilde{v}})$ over $\mathbb{T}^T(Y)$.

Finally, if $q_v \equiv 1 \mod \ell$ then
$$r_{\mathfrak{m}}|_{\Gamma_{\widetilde{v}}} \cong s \oplus (V \circ \mathrm{Art}_{F_{\widetilde{v}}}^{-1}),$$
where s is unramified.

PROOF. This is the analogue of Proposition 3.4.4 of **[CHT08]**, and can be proved exactly in the same way. □

COROLLARY 3.3. *Let Q' denote a finite set of places of F^+, split in F and disjoint from T. Let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of $\mathbb{T}^T_{\mathbf{a},\chi}(U)$ with residue field k, and let $U_1(Q') = \prod_{v\notin Q'} U_v \times \prod_{v\in Q'} U_1(\widetilde{v})$. Denote by $\varphi : \mathbb{T}^{T\cup Q'}_{\mathbf{a},\chi}(U') \to \mathbb{T}^T_{\mathbf{a},\chi}(U)$ the natural map, and let $\mathfrak{m}' = \varphi^{-1}(\mathfrak{m})$, so that $\mathfrak{m}'$ is also non-Eisenstein with residue field k. Then the localized map $\varphi : \mathbb{T}^{T\cup Q'}_{\mathbf{a},\chi}(U_1(Q'))_{\mathfrak{m}'} \to \mathbb{T}^T_{\mathbf{a},\chi}(U)_{\mathfrak{m}}$ is surjective.*

PROOF. It suffices to see that $T_w^{(j)}/1$ is in the image of φ for $j = 1, \ldots, n$ and w a place of F over Q', which follows easily because $r_{\mathfrak{m}} = \varphi \circ r_{\mathfrak{m}'}$, and so
$$T_w^{(j)} = \varphi\left(q_w^{j(1-j)/2}\,\mathrm{Tr}\left(\bigwedge^j r_{\mathfrak{m}'}\right)(\phi_w)\right),$$
where ϕ_w is any lift of Frobenius at w. □

3.2. The main theorem. In this section we will use the Taylor-Wiles method in the version improved by Diamond, Fujiwara, Kisin and Taylor. We will recapitulate the running assumptions made until now, and add a few more. Thus, let F^+ be a totally real field and F/F^+ a totally imaginary quadratic extension. Fix a positive integer n and an odd prime $\ell > n$. Let $K/\mathbb{Q}_\ell$ be a finite extension, let $\overline{K}$ be an algebraic closure of K, and suppose that K is big enough to contain the image of every embedding $F \hookrightarrow \overline{K}$. Let $\mathcal{O}$ be the ring of integers of K, and k its residue field. Let S_ℓ denote the set of places of F^+ above ℓ. Let $\widetilde{S}_\ell$ denote a set of places of F above ℓ such that $\widetilde{S}_\ell \coprod \widetilde{S}_\ell^c$ are all the places above ℓ. We let $\widetilde{I}_\ell$ denote the set of embeddings $F \hookrightarrow K$ which give rise to a place in $\widetilde{S}_\ell$. We will suppose that the following conditions are satisfied.

- F/F^+ is unramified at all finite places;
- ℓ is unramified in F^+;
- every place of S_ℓ is split in F;

Let G be a totally definite unitary group in n variables, attached to the extension F/F^+ such that G_v is quasi-split for every finite place v (cf. Section 2.4 for conditions on n and $[F^+ : \mathbb{Q}]$ to ensure that such a group exists). Choose a lattice in F^+ giving a model for G over $\mathcal{O}_{F^+}$, and fix a basis of the lattice, so that for each split $v = ww^c$, there are two isomorphisms

$$i_w : G_v \longrightarrow \mathrm{GL}_{n/F_w}$$

and

$$i_{w^c} : G_v \longrightarrow \mathrm{GL}_{n/F_{w^c}}$$

taking $G(\mathcal{O}_{F_v^+})$ to $\mathrm{GL}_n(\mathcal{O}_{F_w})$ and $\mathrm{GL}_n(\mathcal{O}_{F_{w^c}})$ respectively.

Let S_a denote a finite, non-empty set of primes of F^+, disjoint from S_ℓ, such that if $v \in S_a$ then

- v splits in F, and
- if v lies above a rational prime p then v is unramified over p and $[F(\zeta_p) : F] > n$.

Let S_r denote a finite set of places of F^+, disjoint from $S_a \cup S_\ell$, such that if $v \in S_r$ then

- v splits in F, and
- $q_v \equiv 1 \mod \ell$.

We will write $T = S_\ell \cup S_a \cup S_r$, and $\widetilde{T} \supset \widetilde{S}_\ell$ for a set of places of F above those of T such that $\widetilde{T} \coprod \widetilde{T}^c$ is the set of all places of F above T. For $S \subset T$, we will write $\widetilde{S}$ to denote the set of $\widetilde{v}$ for $v \in S$. We will fix a compact open subgroup

$$U = \prod_v U_v$$

of $G(\mathbb{A}_{F^+}^\infty)$, such that

- if v is not split in F then U_v is a hyperspecial maximal compact subgroup of $G(F_v^+)$;

- if $v \notin S_a \cup S_r$ splits in F then $U_v = G(\mathcal{O}_{F_v^+})$;
- if $v \in S_r$ then $U_v = \mathrm{Iw}(\widetilde{v})$, and
- if $v \in S_a$ then $U_v = i_{\widetilde{v}}^{-1} \ker(\mathrm{GL}_n(\mathcal{O}_{F_{\widetilde{v}}}) \to \mathrm{GL}_n(k_{\widetilde{v}}))$.

Then, U is sufficiently small (U_v has only one element of finite order if $v \in S_a$) and its projection to $G(F_\ell^+)$ is contained in $G(\mathcal{O}_{F_\ell^+})$. Write

$$U_r = \prod_{v \in S_r} U_v.$$

For any finite set Q of places of F^+, split in F and disjoint from T, we will write $T(Q) = T \cup Q$. Also, we will fix a set of places $\widetilde{T}(Q) \supset \widetilde{T}$ of F over $T(Q)$ as above, for each Q. We will also write

$$U_0(Q) = \prod_{v \notin Q} U_v \times \prod_{v \in Q} U_0(\widetilde{v})$$

and

$$U_1(Q) = \prod_{v \notin Q} U_v \times \prod_{v \in Q} U_1(\widetilde{v}).$$

Thus, $U_0(Q)$ and $U_1(Q)$ are also sufficiently small compact open subgroups of $G(\mathbb{A}_{F^+}^\infty)$.

Fix an element $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,K)}$ such that for every $\tau \in \widetilde{I}_\ell$ we have

- $a_{\tau c,i} = -a_{n+1-i}$ and
- $\ell - 1 - n \geqslant a_{\tau,1} \geqslant \cdots \geqslant a_{\tau,n} \geqslant 0$.

Let $\mathfrak{m} \subset \mathbb{T}^T_{\mathbf{a},1}(U)$ be a non-Eisenstein maximal ideal with residue field equal to k. Write $\mathbb{T} = \mathbb{T}^T_{\mathbf{a},1}(U)_\mathfrak{m}$. Consider the representation

$$\overline{r}_\mathfrak{m} : \mathrm{Gal}(\overline{F}/F^+) \to \mathcal{G}_n(k)$$

and its lifting

$$r_\mathfrak{m} : \mathrm{Gal}(\overline{F}/F^+) \to \mathcal{G}_n(\mathbb{T})$$

given by Proposition 3.2. For $v \in T$, denote by $\overline{r}_{\mathfrak{m},v}$ the restriction of $\overline{r}_\mathfrak{m}$ to a decomposition group $\Gamma_{\widetilde{v}}$ at $\widetilde{v}$. We will *assume* that $\overline{r}_\mathfrak{m}$ has the following properties.

- $\overline{r}_\mathfrak{m}(\mathrm{Gal}(\overline{F}/F^+(\zeta_\ell)))$ is big (for the definition of bigness, see 0.6);
- if $v \in S_r$ then $\overline{r}_{\mathfrak{m},v}$ is the trivial representation of $\Gamma_{\widetilde{v}}$, and
- if $v \in S_a$ then $\overline{r}_\mathfrak{m}$ is unramified at v and

$$H^0(\Gamma_{\widetilde{v}}, (\mathrm{ad}\, \overline{r}_\mathfrak{m})(1)) = 0.$$

We will use the Galois deformation theory developed in Section 2 of **[CHT08]**, to where we refer the reader for the definitions and results. Consider the global deformation problem

$$\mathcal{S} = (F/F^+, T, \widetilde{T}, \mathcal{O}, \overline{r}_\mathfrak{m}, \epsilon^{1-n}\delta_{F/F^+}^{\mu_\mathfrak{m}}, \{\mathcal{D}_v\}_{v \in T}),$$

where the local deformation problems $\mathscr{D}_v$ are as follows. For $v \in T$, we denote by

$$r_v^{\text{univ}} : \Gamma_{\tilde{v}} \to \mathrm{GL}_n(R_v^{\text{loc}})$$

the universal lifting ring of $\overline{r}_{\mathfrak{m},v}$, and by $\mathscr{I}_v \subset R_v^{\text{loc}}$ the ideal corresponding to $\mathscr{D}_v$.

- For $v \in S_a$, $\mathscr{D}_v$ consists of all lifts of $\overline{r}_{\mathfrak{m},v}$, and thus $\mathscr{I}_v = 0$.
- For $v \in S_\ell$, $\mathscr{D}_v$ consist of all lifts whose artinian quotients all arise from torsion Fontaine-Laffaille modules, as in Section 2.4.1 of **[CHT08]**.
- For $v \in S_r$, $\mathscr{D}_v$ corresponds to the ideal $\mathscr{I}_v^{(1,1,\dots,1)}$ of R_v^{loc}, as in Section 3 of **[Tay08]**. Thus, $\mathscr{D}_v$ consists of all the liftings $r : \Gamma_{\tilde{v}} \to \mathrm{GL}_n(A)$ such that for every σ in the inertia subgroup $I_{\tilde{v}}$, the characteristic polynomial of $r(\sigma)$ is

$$\prod_{i=1}^{n}(X-1).$$

Let

$$r_{\mathscr{S}}^{\text{univ}} : \mathrm{Gal}(\overline{F}/F^+) \to \mathscr{G}_n(R_{\mathscr{S}}^{\text{univ}})$$

denote the universal deformation of $\overline{r}_{\mathfrak{m}}$ of type $\mathscr{S}$. By Proposition 3.2, $r_{\mathfrak{m}}$ gives a lifting of $\overline{r}_{\mathfrak{m}}$ which is of type $\mathscr{S}$; this gives rise to a surjection

$$R_{\mathscr{S}}^{\text{univ}} \longrightarrow \mathbb{T}.$$

Let $H = S_{\mathbf{a},1}(U, \mathscr{O})_{\mathfrak{m}}$. This is a $\mathbb{T}$-module, and under the above map, a $R_{\mathscr{S}}^{\text{univ}}$-module. Our main result is the following.

THEOREM 3.4. *Keep the notation and assumptions of the start of this section. Then*

$$(R_{\mathscr{S}}^{\text{univ}})^{\text{red}} \simeq \mathbb{T}.$$

Moreover, $\mu_{\mathfrak{m}} \equiv n \mod 2$.

PROOF. The proof is essentially the same as Taylor's (**[Tay08]**), except that here there are no primes $S(B)_1$ and $S(B)_2$, in his notation. One has just to note that his argument is still valid in our simpler case. The idea is to use Kisin's version (**[Kis09]**) of the Taylor-Wiles method in the following way, in order to avoid dealing with non-minimal deformations separately. There are essentially two moduli problems to consider at places in S_r. One of them consists in considering all the characters χ_v to be trivial. This is the case in which we are ultimately interested, but the local deformation rings are not so well behaved (for example, they are not irreducible). We call this the *degenerate case*. On the other hand, we can also consider the characters χ_v in such a way that $\chi_{v,i} \neq \chi_{v,j}$ for all $v \in S_r$ and all $i \neq j$. This is the *non-degenerate case*, and we can always consider such a set of characters by our assumption that $\ell > n$. Note that both problems are equal modulo ℓ. The Taylor-Wiles-Kisin method doesn't work with the first moduli problem, but it works fine in the non-degenerate case. Taylor's idea is to apply all the steps of the method simultaneosly for the degenerate and non-degenerate cases, and obtain the final conclusion of the theorem by means of comparing both processes modulo λ, and using the fact that in the degenerate case, even if the local deformation ring is not irreducible, every prime ideal which is minimal over λ contains a unique minimal prime, and this suffices to proof what we want. We will reproduce most of the argument in the following pages. What we will prove in the end is that H is a nearly faithful $R^{\mathrm{univ}}_{\mathscr{S}}$-module, which by definition means that the ideal $\mathrm{Ann}_{R^{\mathrm{univ}}_{\mathscr{S}}}(H)$ is nilpotent. Since $\mathbb{T}$ is reduced, this proves the main statement of the theorem.

We will be working with several deformation problems at a time. Consider a set Q of finite set of places of F^+, disjoint from T, such that if $v \in Q$, then

- v splits as ww^c in F,
- $q_v \equiv 1 \mod \ell$, and
- $\overline{r}_{\mathfrak{m},v} = \overline{\psi}_v \oplus \overline{s}_v$, with $\dim \overline{\psi}_v = 1$ and such that $\overline{s}_v$ does not contain $\overline{\psi}_v$ as a sub-quotient.

Let $T(Q)$ and $\widetilde{T}(Q)$ be as in the start of the section. Also, let $\{\chi_v : \mathrm{Iw}(\widetilde{v}) / \mathrm{Iw}_1(\widetilde{v}) \to \mathscr{O}^\times\}_{v \in S_r}$ be a set of characters of order dividing ℓ. To facilitate the notation, we will write $\chi_v = (\chi_{v,1}, \ldots, \chi_{v,n})$ and $\chi = \{\chi_v\}_{v \in S_r}$. Consider the deformation problem given by

$$\mathscr{S}_{\chi,Q} = (F/F^+, T(Q), \widetilde{T}(Q), \mathscr{O}, \overline{r}_{\mathfrak{m}}, \epsilon^{1-n}\delta_{F/F^+}^{\mu_{\mathfrak{m}}}, \{\mathscr{D}'_v\}_{v \in T(Q)}),$$

where:

- for $v \in S_a \cup S_\ell$, $\mathscr{D}'_v = \mathscr{D}_v$;
- for $v \in S_r$, $\mathscr{D}'_v$ consists of all the liftings $r : \Gamma_{\widetilde{v}} \to \mathrm{GL}_n(A)$ such that the characteristic polynomial of $r(\sigma)$ for $\sigma \in I_{\widetilde{v}}$ is
$$\prod_{i=1}^{n}(X - \chi_{v,i}^{-1}(\mathrm{Art}_{F_{\widetilde{v}}}^{-1}\sigma))$$
(see Section 3 of [**Tay08**]).
- for $v \in Q$, $\mathscr{D}'_v$ consists of all Taylor-Wiles liftings of $\overline{r}_{\mathfrak{m},v}$, as in Section 2.4.6 of [**CHT08**]. More precisely, $\mathscr{D}'_v$ consists of all the liftings $r : \Gamma_{\widetilde{v}} \to \mathrm{GL}_n(A)$ which are conjugate to one of the form $\psi_v \oplus s_v$ with ψ_v a lift of $\overline{\psi}_v$ and s_v an unramified lift of $\overline{s}_v$.

Denote by $\mathscr{I}_v^{\chi_v}$ the corresponding ideal of R_v^{loc} for every $v \in T(Q)$. Let

$$r^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}} : \mathrm{Gal}(\overline{F}/F^+) \to \mathscr{G}_n(R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}})$$

denote the universal deformation of $\overline{r}$ of type $\mathscr{S}_{\chi,Q}$, and let

$$r^{\square_T}_{\mathscr{S}_{\chi,Q}} : \mathrm{Gal}(\overline{F}/F^+) \to \mathscr{G}_n(R^{\square_T}_{\mathscr{S}_{\chi,Q}})$$

denote the universal T-framed deformation of $\overline{r}$ of type $\mathscr{S}_{\chi,Q}$ (see [**CHT08**, 2.2.7] for the definition of T-framed deformations; note that it depends on $\widetilde{T}$). Thus, by definition of the deformation problems, we have that $R^{\mathrm{univ}}_{\mathscr{S}_{1,\varnothing}} = R^{\mathrm{univ}}_{\mathscr{S}}$. As we claimed above, both problems are equal modulo ℓ. We have isomorphisms

$$R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}}/\lambda \cong R^{\mathrm{univ}}_{\mathscr{S}_{1,Q}}/\lambda \tag{3.2.1}$$

and

$$R^{\square_T}_{\mathscr{S}_{\chi,Q}}/\lambda \cong R^{\square_T}_{\mathscr{S}_{1,Q}}/\lambda, \tag{3.2.2}$$

compatible with the natural commutative diagrams

$$\begin{tikzcd} R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}} \arrow[r, two heads] \arrow[d] & R^{\mathrm{univ}}_{\mathscr{S}_{\chi,\varnothing}} \arrow[d] \\ R^{\square_T}_{\mathscr{S}_{\chi,Q}} \arrow[r, two heads] & R^{\square_T}_{\mathscr{S}_{\chi,\varnothing}} \end{tikzcd}$$

and

$$\begin{tikzcd} R^{\mathrm{univ}}_{\mathscr{S}_{1,Q}} \arrow[r, two heads] \arrow[d] & R^{\mathrm{univ}}_{\mathscr{S}_{1,\varnothing}} \arrow[d] \\ R^{\square_T}_{\mathscr{S}_{1,Q}} \arrow[r, two heads] & R^{\square_T}_{\mathscr{S}_{1,\varnothing}} \end{tikzcd}$$

Also, let

$$R^{\mathrm{loc}}_{\chi,T} = \widehat{\bigotimes}_{v\in T} R^{\mathrm{loc}}_v / \mathscr{I}_v^{\chi_v}.$$

Then

$$R^{\mathrm{loc}}_{\chi,T}/\lambda \cong R^{\mathrm{loc}}_{1,T}/\lambda. \tag{3.2.3}$$

To any T-framed deformation of type $\mathscr{S}_{\chi,Q}$ and any $v \in T$ we can associate a lifting of $\bar{r}_{\mathfrak{m},v}$ of type $\mathscr{D}_v$, and hence there are natural maps

$$R^{\mathrm{loc}}_{\chi,T} \longrightarrow R^{\square_T}_{\mathscr{S}_{\chi,Q}}$$

which modulo λ are compatible with the identifications (3.2.3) and (3.2.2).

Let $\mathscr{T} = \mathscr{O}[[X_{v,i,j}]]_{v\in T; i,j=1,\dots,n}$. Then a choice of a lifting $r^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}}$ of $\bar{r}_{\mathfrak{m}}$ over $R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}}$ representing the universal deformation of type $\mathscr{S}_{\chi,Q}$ gives rise to an isomorphism of $R^{\mathrm{univ}}_{\mathscr{S},Q}$-algebras

$$R^{\square_T}_{\mathscr{S}_{\chi,Q}} \simeq R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}} \hat{\otimes}_{\mathscr{O}} \mathscr{T}, \tag{3.2.4}$$

so that

$$(r^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}}; \{1_n + (X_{v,i,j})\}_{v\in T})$$

represents the universal T-framed deformation of type $\mathscr{S}_{\chi,Q}$ (see Proposition 2.2.9 of [**CHT08**]). Moreover, we can choose the liftings $r^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}}$ so that

$$r^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}} \otimes_{\mathscr{O}} k = r^{\mathrm{univ}}_{\mathscr{S}_{1,Q}} \otimes_{\mathscr{O}} k$$

under the natural identifications (3.2.1). Then the isomorphisms (3.2.4) for χ and 1 are compatible with the identifications (3.2.2) and (3.2.1).

For $v \in Q$, let ψ_v denote the lifting of $\overline{\psi}_{\tilde{v}}$ to $(R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}})^\times$ given by the lifting $r^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}}$. Also, write Δ_Q for the maximal ℓ-power order quotient of $\prod_{v\in Q} k_{\tilde{v}}^\times$, and let $\mathfrak{a}_Q$ denote the ideal of $\mathscr{T}[\Delta_Q]$ generated by the augmentation ideal of $\mathscr{O}[\Delta_Q]$ and by the $X_{v,i,j}$ for $v \in T$ and $i, j = 1, \dots, n$. Since the primes of Q are different from ℓ and $\overline{\psi}_{\tilde{v}}$ is unramified, ψ_v is tamely ramified, and then

$$\prod_{v \in Q} (\psi_v \circ \mathrm{Art}_{F_{\tilde{v}}}) : \Delta_Q \longrightarrow (R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}})^\times$$

makes $R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}}$ an $\mathscr{O}[\Delta_Q]$-algebra. This algebra structure is compatible with the identifications (3.2.1), because we chose the liftings $r^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q}}$ and $r^{\mathrm{univ}}_{\mathscr{S}_{1,Q}}$ compatibly. Via the isomorphisms (3.2.4), $R^{\square T}_{\mathscr{S}_{\chi,Q}}$ are $\mathscr{T}[\Delta_Q]$-algebras, which are compatible modulo λ for the different choices of χ. Finally, we have an isomorphism

$$R^{\square T}_{\mathscr{S}_{\chi,Q}} / \mathfrak{a}_Q \simeq R^{\mathrm{univ}}_{\mathscr{S}_{\chi,\varnothing}}, \tag{3.2.5}$$

compatible with the identifications (3.2.2) and (3.2.1), the last one with $Q = \varnothing$.

Note that since

$$S_{\mathbf{a},1}(U, k) = S_{\mathbf{a},\chi}(U, k)$$

we can find a maximal ideal $\mathfrak{m}_{\chi,\varnothing} \subset \mathbb{T}^T_{\mathbf{a},\chi}(U)$ with residue field k such that for a prime w of F split over a prime $v \notin T$ of F^+, the Hecke operators $T^{(j)}_w$ have the same image in $\mathbb{T}^T_{\mathbf{a},\chi}(U)/\mathfrak{m}_{\chi,\varnothing} = k$ as in $\mathbb{T}^T_{\mathbf{a},1}(U)/\mathfrak{m} = k$. It follows that $\bar{r}_{\mathfrak{m}_{\chi,\varnothing}} \cong \bar{r}_{\mathfrak{m}}$, and in particular $\mathfrak{m}_{\chi,\varnothing}$ is non-Eisenstein. We define $\mathfrak{m}_{\chi,Q} \subset \mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))$ as the preimage of $\mathfrak{m}_{\chi,\varnothing}$ under the natural map

$$\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q)) \twoheadrightarrow \mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_0(Q)) \twoheadrightarrow \mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U) \hookrightarrow \mathbb{T}^{T}_{\mathbf{a},\chi}(U).$$

Then $\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))/\mathfrak{m}_{\chi,Q} = k$, and if a prime w of F splits over a prime $v \notin T(Q)$ of F^+, then the Hecke operators $T^{(j)}_w$ have the same image in $\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))/\mathfrak{m}_{\chi,Q} = k$ as in $\mathbb{T}^T_{\mathbf{a},1}(U)/\mathfrak{m} = k$. Hence, $\bar{r}_{\mathfrak{m}_{\chi,Q}} \cong \bar{r}_{\mathfrak{m}}$ and $\mathfrak{m}_{\chi,Q}$ is non-Eisenstein. Let

$$r_{\mathfrak{m}_{\chi,Q}} : \mathrm{Gal}(\overline{F}/F^+) \to \mathscr{G}_n(\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))_{\mathfrak{m}_{\chi,Q}})$$

be the continuous representation attached to $\mathfrak{m}_{\chi,Q}$ as in Proposition 3.2. Write $\mathbb{T}_\chi = \mathbb{T}^T_{\mathbf{a},\chi}(U)_{\mathfrak{m}_{\chi,\varnothing}}$ and $H_\chi = S_{\mathbf{a},\chi}(U, \mathscr{O})_{\mathfrak{m}_{\chi,\varnothing}}$. We have the following natural surjections

$$\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))_{\mathfrak{m}_{\chi,Q}} \twoheadrightarrow \mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_0(Q))_{\mathfrak{m}_{\chi,Q}} \twoheadrightarrow \mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U)_{\mathfrak{m}_{\chi,Q}} = \mathbb{T}_\chi. \tag{3.2.6}$$

The last equality follows easily from Corollary 3.3.

For each $v \in Q$, choose $\phi_{\tilde{v}} \in \Gamma_{\tilde{v}}$ a lift of $\mathrm{Frob}_{\tilde{v}}$, and let $\varpi_{\tilde{v}} \in F^\times_{\tilde{v}}$ be the uniformizer corresponding to $\phi_{\tilde{v}}$ via $\mathrm{Art}_{F_{\tilde{v}}}$. Let

$$P_{\tilde{v}} \in \mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))_{\mathfrak{m}_{\chi,Q}}[X]$$

denote the characteristic polynomial of $r_{\mathfrak{m}_{\chi,Q}}(\phi_{\tilde{v}})$. Since $\overline{\psi}_v(\phi_{\tilde{v}})$ is a simple root of the characteristic polynomial of $\bar{r}_{\mathfrak{m}}(\phi_{\tilde{v}})$, by Hensel's lemma, there exists a unique root

$A_{\tilde{v}} \in \mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))_{\mathfrak{m}_{\chi,Q}}$ of $P_{\tilde{v}}$ lifting $\overline{\psi}_v(\phi_{\tilde{v}})$. Thus, there is a factorisation

$$P_{\tilde{v}}(X) = (X - A_{\tilde{v}})Q_{\tilde{v}}(X)$$

over $\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))_{\mathfrak{m}_{\chi,Q}}$, where $Q_{\tilde{v}}(A_{\tilde{v}}) \in \mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))^{\times}_{\mathfrak{m}_{\chi,Q}}$. By part (i) of Proposition 1.7 and Lemma 1.9, $P_{\tilde{v}}(V_{\varpi_{\tilde{v}},1}) = 0$ on $S_{\mathbf{a},\chi}(U_1(Q),\mathcal{O})_{\mathfrak{m}_{\chi,Q}}$. For $i = 0,1$, let

$$H_{i,\chi,Q} = \left(\prod_{v\in Q} Q_{\tilde{v}}(V_{\varpi_{\tilde{v}},i})\right) S_{\mathbf{a},\chi}(U_i(Q),\mathcal{O})_{\mathfrak{m}_{\chi,Q}} \subset S_{\mathbf{a},\chi}(U_i(Q),\mathcal{O})_{\mathfrak{m}_{\chi,Q}},$$

and let $\mathbb{T}_{i,\chi,Q}$ denote the image of $\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))_{\mathfrak{m}_{\chi,Q}}$ in $\mathrm{End}_{\mathcal{O}}(H_{i,\chi,Q})$. We see that $H_{1,\chi,Q}$ is a direct summand of $S_{\mathbf{a},\chi}(U_1(Q),\mathcal{O})$ as a $\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))$-module. Also, we have an isomorphism

$$\left(\prod_{v\in Q} Q_{\tilde{v}}(V_{\overline{\varpi}_{\tilde{v}},0})\right) : H_{\chi} \cong H_{0,\chi,Q}.$$

This can be proved using Proposition 1.7 and Lemmas 1.9 and 1.10, as in **[CHT08**, 3.2.2].

For all $v \in Q$, $V_{\varpi_{\tilde{v}},1} = A_{\tilde{v}}$ on $H_{1,\chi,Q}$. By part (vii) of Proposition 3.2, for each $v \in Q$ there is a character with open kernel

$$V_v : F^{\times}_{\tilde{v}} \longrightarrow \mathbb{T}^{\times}_{1,\chi,Q}$$

such that

- if $\alpha \in \mathcal{O}_{F_{\tilde{v}}}$ is non-zero, then $V_{\alpha,1} = V_v(\alpha)$ on $H_{1,\chi,Q}$ and
- $(r_{\mathfrak{m}_{\chi,Q}} \otimes \mathbb{T}_{1,\chi,Q})|_{\Gamma_{\tilde{v}}} \cong s_v \oplus (V_v \circ \mathrm{Art}^{-1}_{F_{\tilde{v}}})$, where s_v is unramified.

It is clear that $V_v \circ \mathrm{Art}^{-1}_{F_{\tilde{v}}}$ is a lifting of $\overline{\psi}_v$ and s_v is a lifting of $\overline{s}_v$. It follows by (v) and (vi) of the same proposition that $r_{\mathfrak{m}_{\chi,Q}} \otimes \mathbb{T}_{1,\chi,Q}$ gives rise to a deformation of $\overline{r}_{\mathfrak{m}}$ of type $\mathcal{S}_{\chi,Q}$, and thus to a surjection

$$R^{\mathrm{univ}}_{\mathcal{S}_{\chi,Q}} \twoheadrightarrow \mathbb{T}_{1,\chi,Q},$$

such that the composition

$$\prod_{v\in Q} \mathcal{O}^{\times}_{F_{\tilde{v}}} \twoheadrightarrow \Delta_Q \to (R^{\mathrm{univ}}_{\mathcal{S}_{\chi,Q}})^{\times} \to \mathbb{T}^{\times}_{1,\chi,Q}$$

coincides with $\prod_{v\in Q} V_v$. We then have that $H_{1,\chi,Q}$ is an $R^{\mathrm{univ}}_{\mathcal{S}_{\chi,Q}}$-module, and we set

$$H^{\square_T}_{1,\chi,Q} = H_{1,\chi,Q} \otimes_{R^{\mathrm{univ}}_{\mathcal{S}_{\chi,Q}}} R^{\square_T}_{\mathcal{S}_{\chi,Q}} = H_{1,\chi,Q} \otimes_{\mathcal{O}} \mathcal{T}.$$

Since $\ker(\prod_{v\in Q} k^{\times}_{\tilde{v}} \to \Delta_Q)$ acts trivially on $H_{1,\chi,Q}$ and $H_{1,\chi,Q}$ is a $\mathbb{T}^{T(Q)}_{\mathbf{a},\chi}(U_1(Q))$-direct summand of $S_{\mathbf{a},\chi}(U_1(Q),\mathcal{O})$, Lemma 2.1 implies that $H_{1,\chi,Q}$ is a finite free $\mathcal{O}[\Delta_Q]$-module, and that

$$(H_{1,\chi,Q})_{\Delta_Q} \cong H_{0,\chi,Q} \cong H_{\chi}.$$

Since U is sufficiently small, we get isomorphisms

$$S_{\mathbf{a},\chi}(U,\mathscr{O})\otimes_{\mathscr{O}} k \cong S_{\mathbf{a},\chi}(U,k) = S_{\mathbf{a},1}(U,k) \cong S_{\mathbf{a},1}(U,\mathscr{O})\otimes_{\mathscr{O}} k$$

and

$$S_{\mathbf{a},\chi}(U_1(Q),\mathscr{O})\otimes_{\mathscr{O}} k \cong S_{\mathbf{a},\chi}(U_1(Q),k) = S_{\mathbf{a},1}(U_1(Q),k) \cong S_{\mathbf{a},1}(U_1(Q),\mathscr{O})\otimes_{\mathscr{O}} k.$$

Thus we get identifications

$$H_\chi/\lambda \cong H_1/\lambda,$$
$$H_{1,\chi,Q}/\lambda \cong H_{1,1,Q}/\lambda$$

and

$$H^{\square_T}_{1,\chi,Q}/\lambda \cong H^{\square_T}_{1,1,Q}/\lambda,$$

compatible with all the pertinent identifications modulo λ made before.

Let

$$\varepsilon_\infty = (1-(-1)^{\mu_{\mathfrak{m}}-n})/2$$

and

$$q_0 = [F^+:\mathbb{Q}]n(n-1)/2 + [F^+:\mathbb{Q}]n\varepsilon_\infty.$$

By Proposition 2.5.9 of **[CHT08]**, there is an integer $q \geqslant q_0$, such that for every natural number N, we can find a set of primes Q_N (and a set of corresponding $\overline{\psi}_v$ and $\bar{s}_v$ for $\bar{r}_{\mathfrak{m}}$) such that

- $\#Q_N = q$;
- for $v \in Q_N$, $q_v \equiv 1 (\mathrm{mod}\ \ell^N)$ and
- $R^{\square_T}_{\mathscr{S}_{1,Q_N}}$ can be topologically generated over $R^{\mathrm{loc}}_{1,T}$ by $q' = q - q_0$ elements.

Define

$$R^{\square_T}_{\chi,\infty} = R^{\mathrm{loc}}_{\chi,T}[[Y_1,\dots,Y_{q'}]].$$

Then there is a surjection

$$R^{\square_T}_{1,\infty} \twoheadrightarrow R^{\square_T}_{\mathscr{S}_{1,Q_N}}$$

extending the natural map $R^{\mathrm{loc}}_{1,T} \to R^{\square_T}_{\mathscr{S}_{1,Q_N}}$. Reducing modulo λ and lifting the obtained surjection, via the identifications

$$R^{\square_T}_{\chi,\infty}/\lambda \simeq R^{\square_T}_{1,\infty}/\lambda,$$

we obtain a surjection

$$R^{\square_T}_{\chi,\infty} \twoheadrightarrow R^{\square_T}_{\mathscr{S}_{\chi,Q_N}}$$

extending the natural map $R^{\mathrm{loc}}_{\chi,T} \to R^{\square_T}_{\mathscr{S}_{\chi,Q_N}}$.

For $v \in S_a$, $R^{\mathrm{loc}}_v/\mathscr{I}^{\chi_v}_v$ is a power series ring over $\mathscr{O}$ in n^2 variables (see Lemma 2.4.9 of **[CHT08]**), and for $v \in S_\ell$ it is a power series ring over $\mathscr{O}$ in $n^2 + [F_{\tilde{v}}:\mathbb{Q}_\ell]n(n-1)/2$ variables (see Corollary 2.4.3 of *loc. cit.*).

Suppose that $\chi_{v,i} \neq \chi_{v,j}$ for every $v \in S_r$ and every $i,j = 1,\dots,n$ with $i \neq j$. Then, by Proposition 3.1 of **[Tay08]**, for every $v \in S_r$, $R^{\mathrm{loc}}_v/\mathscr{I}^{\chi_v}_v$ is irreducible of dimension n^2+1 and its generic point has characteristic zero. It follows that $(R^{\mathrm{loc}}_v/\mathscr{I}^{\chi_v}_v)^{\mathrm{red}}$ is geometrically integral (in the sense that $(R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v})^{\mathrm{red}} \otimes_{\mathscr{O}} \mathscr{O}'$ is an integral domain for every finite extension K'/K, where $\mathscr{O}'$ is the ring of integers of K') and flat over $\mathscr{O}$. Moreover, by part 3. of Lemma 3.3 of **[BLGHT]**,

$$(R_{\chi,\infty}^{\square_T})^{\mathrm{red}} \simeq \left(\left(\widehat{\bigotimes}_{v\in S_r}(R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v})^{\mathrm{red}}\right)\widehat{\bigotimes}\left(\widehat{\bigotimes}_{v\in S_a\cup S_\ell}R_v^{\mathrm{loc}}/\mathscr{I}_v\right)\right)[[Y_1,\ldots,Y_{q'}]],$$

and the same part of that lemma implies that $(R_{\chi,\infty}^{\square_T})^{\mathrm{red}}$ is geometrically integral. We conclude that in the non-degenerate case, $R_{\chi,\infty}^{\square_T}$ is irreducible, and, by part 2., its Krull dimension is

$$1+q+n^2\#T-[F^+:\mathbb{Q}]n\varepsilon_\infty.$$

Suppose now that we are in the degenerate case, that is, $\chi_v = 1$ for every $v \in S_r$. Then (see Proposition 3.1 of **[Tay08]**) for every such v, $R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v}$ is pure of dimension n^2+1, its generic points have characteristic zero, and every prime of $R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v}$ which is minimal over $\lambda(R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v})$ contains a unique minimal prime. After eventually replacing K by a finite extension K' (which we are allowed to do since the main theorem for one K implies the same theorem for every K'), $R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v}$ satisfies that for every prime ideal $\mathfrak{p}$ which is minimal (resp. every prime ideal $\mathfrak{q}$ which is minimal over $\lambda(R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v})$), the quotient $(R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v})/\mathfrak{p}$ (resp. $(R_v^{\mathrm{loc}}/\mathscr{I}_v^{\chi_v})/\mathfrak{q}$) is geometrically integral. It follows then by parts 2., 5. and 7. of Lemma 3.3 of **[BLGHT]** that every prime ideal of $R_{1,\infty}^{\square_T}$ which is minimal over $\lambda R_{1,\infty}^{\square_T}$ contains a unique minimal prime, the generic points of $R_{1,\infty}^{\square_T}$ have characteristic zero and $R_{1,\infty}^{\square_T}$ is pure.

Let $\Delta_\infty = \mathbb{Z}_\ell^q$, $S_\infty = \mathscr{T}[[\Delta_\infty]]$ and $\mathfrak{a} = \ker(S_\infty \twoheadrightarrow \mathscr{O})$, where the map sends Δ_∞ to 1 and the variables $X_{v,i,j}$ to 0. Thus, S_∞ is isomorphic to a power series ring over $\mathscr{O}$ in $q+n^2\#T$ variables. For every N, choose a surjection

$$\Delta_\infty \twoheadrightarrow \Delta_{Q_N}.$$

We have an induced map on completed group algebras

$$\mathscr{O}[[\Delta_\infty]] \twoheadrightarrow \mathscr{O}[\Delta_{Q_N}].$$

and thus a map

$$S_\infty \twoheadrightarrow \mathscr{T}[\Delta_{Q_N}] \to R_{\mathscr{S}_{\chi,Q_N}}^{\square_T} \tag{3.2.7}$$

which makes $R_{\mathscr{S}_{\chi,Q_N}}^{\square_T}$ an algebra over S_∞. The map $S_\infty \twoheadrightarrow \mathscr{T}[\Delta_{Q_N}]$ sends the ideal $\mathfrak{a}$ to $\mathfrak{a}_{Q_N}$. Let $\mathfrak{c}_N = \ker(S_\infty \twoheadrightarrow \mathscr{T}[\Delta_{Q_N}])$. Note that every open ideal of S_∞ contains $\mathfrak{c}_N$ for some N. The following properties hold.

- $H_{1,\chi,Q_N}^{\square_T}$ is finite free over $S_\infty/\mathfrak{c}_N$.
- $R_{\mathscr{S}_{\chi,Q_N}}^{\square_T}/\mathfrak{a} \simeq R_{\mathscr{S}_{\chi,\varnothing}}^{\mathrm{univ}}$.
- $H_{1,\chi,Q_N}^{\square_T}/\mathfrak{a} \simeq H_\chi$.

In what follows, we will use that we can patch the $R_{\mathscr{S}_{\chi,Q_N}}^{\square_T}$ to obtain in the limit a copy of $R_{\chi,\infty}^{\square_T}$, and simultaneously patch the H_{1,χ,Q_N} to form a module over $R_{\chi,\infty}^{\square_T}$, finite free over S_∞. The patching construction is carried on in exactly the same way as in

[Tay08]. The outcome of this process is a family of $R^{\square_T}_{\chi,\infty}\widehat{\otimes}_{\mathscr{O}}S_\infty$-modules $H^{\square_T}_{1,\chi,\infty}$ with the following properties.

(1) They are finite free over S_∞, and the S_∞-action factors through $R^{\square_T}_{\chi,\infty}$, in such a way that the obtained maps $S_\infty \to R^{\square_T}_{\chi,\infty} \twoheadrightarrow R^{\square_T}_{\mathscr{S}_{\chi,Q_N}}$ are the maps defined in (3.2.7) for every N; in particular, there is a surjection
$$R^{\square_T}_{\chi,\infty}/\mathfrak{a} \twoheadrightarrow R^{\mathrm{univ}}_{\mathscr{S}_{\chi,Q_N}}/\mathfrak{a} = R^{\mathrm{univ}}_{\mathscr{S}_{\chi,\varnothing}}.$$
(2) There are isomorphism $H^{\square_T}_{1,\chi,\infty}/\lambda \simeq H^{\square_T}_{1,1,\infty}/\lambda$ of $R^{\square_T}_{\chi,\infty}/\lambda \simeq R^{\square_T}_{1,\infty}/\lambda$-modules.

(3) There are isomorphisms $H^{\square_T}_{1,\chi,\infty}/\mathfrak{a} \simeq H_\chi$ of $R^{\square_T}_{\chi,\infty}/\mathfrak{a}$-modules, where we see H_χ as a module over $R^{\square_T}_{\chi,\infty}/\mathfrak{a}$ by means of the map in (1). Moreover, these isomorphisms agree modulo λ via the identifications of (2).

Let us place ourselves in the non-degenerate case. That is, let us choose the characters χ such that $\chi_{v,i} \neq \chi_{v,j}$ for every $v \in S_r$ and every $i \neq j$. This is possible because $\ell > n$ and $q_v \equiv 1 (\mathrm{mod}\, \ell)$ for $v \in S_r$. Since the action of S_∞ on $H^{\square_T}_{1,\chi,\infty}$ factors through $R^{\square_T}_{\chi,\infty}$,

$$\mathrm{depth}_{R^{\square_T}_{\chi,\infty}}(H^{\square_T}_{1,\chi,\infty}) \geqslant \mathrm{depth}_{S_\infty}(H^{\square_T}_{1,\chi,\infty}). \tag{3.2.8}$$

Also, since $H^{\square_T}_{1,\chi,\infty}$ is finite free over S_∞, which is a Cohen-Macaulay ring, by the Auslander-Buchsbaum formula we have that

$$\mathrm{depth}_{S_\infty}(H^{\square_T}_{1,\chi,\infty}) = \dim S_\infty = 1 + q + n^2\#T. \tag{3.2.9}$$

Since the depth of a module is at most its Krull dimension, by equations (3.2.8) and (3.2.9) we obtain that

$$\dim\left(R^{\square_T}_{\chi,\infty}/\operatorname{Ann}_{R^{\square_T}_{\chi,\infty}}(H^{\square_T}_{1,\chi,\infty})\right) \geqslant 1 + q + n^2\#T. \tag{3.2.10}$$

Recall that $R^{\square_T}_{\chi,\infty}$ is irreducible of dimension

$$1 + q + n^2\#T - [F^+ : \mathbb{Q}]n\varepsilon_\infty. \tag{3.2.11}$$

Then, (3.2.10), (3.2.11) and Lemma 2.3 of **[Tay08]** imply that $\varepsilon = 0$ (that is, $\mu_{\mathfrak{m}} \equiv n (\mathrm{mod}\, 2)$) and that $H^{\square_T}_{1,\chi,\infty}$ is a nearly faithful $R^{\square_T}_{\chi,\infty}$-module. This implies in turn that $H^{\square_T}_{1,\chi,\infty}/\lambda \simeq H^{\square_T}_{1,1,\infty}/\lambda$ is a nearly faithful $R^{\square_T}_{\chi,\infty}/\lambda \simeq R^{\square_T}_{1,\infty}/\lambda$-module (this follows from Nakayama's Lemma, as in Lemma 2.2 of **[Tay08]**). Since the generic points of $R^{\square_T}_{1,\infty}$ have characteristic zero, $R^{\square_T}_{1,\infty}$ is pure and every prime of $R^{\square_T}_{1,\infty}$ which is minimal over $\lambda R^{\square_T}_{1,\infty}$ contains a unique minimal prime of $R^{\square_T}_{1,\infty}$, the same lemma implies that $H^{\square_T}_{1,1,\infty}$ is a nearly faithful $R^{\square_T}_{1,\infty}$-module. Finally, using the same Lemma again, this implies that $H^{\square_T}_{1,1,\infty}/\mathfrak{a} \simeq H$ is a nearly faithful $R^{\square_T}_{1,\infty}/\mathfrak{a}$-module, and since $R^{\square_T}_{1,\infty}/\mathfrak{a} \twoheadrightarrow R^{\mathrm{univ}}_{\mathscr{S}}$, H is a nearly faithful $R^{\mathrm{univ}}_{\mathscr{S}}$-module. ☐

4. The main theorems

In this section we apply the results of the previous sections to prove modularity lifting theorems for GL_n. We deal first with the case of a totally imaginary field F.

THEOREM 4.1. *Let F^+ be a totally real field, and F a totally imaginary quadratic extension of F^+. Let $n \geqslant 1$ be an integer and $\ell > n$ be a prime number, unramified in F. Let*

$$r : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

be a continuous irreducible representation with the following properties. Let $\bar{r}$ denote the semisimplification of the reduction of r.

(i) $r^c \cong r^\vee(1-n)$.
(ii) r is unramified at all but finitely many primes.
(iii) For every place $v|\ell$ of F, $r|_{\Gamma_v}$ is crystalline.
(iv) There is an element $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F,\overline{\mathbb{Q}}_\ell)}$ such that
- *for all $\tau \in \mathrm{Hom}(F^+, \overline{\mathbb{Q}}_\ell)$, we have either*
$$\ell - 1 - n \geqslant a_{\tau,1} \geqslant \cdots \geqslant a_{\tau,n} \geqslant 0$$
or
$$\ell - 1 - n \geqslant a_{\tau c,1} \geqslant \cdots \geqslant a_{\tau c,n} \geqslant 0;$$
- *for all $\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_\ell)$ and every $i = 1, \ldots, n$,*
$$a_{\tau c,i} = -a_{\tau,n+1-i}.$$
- *for all $\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_\ell)$ giving rise to a prime $w|\ell$,*
$$\mathrm{HT}_\tau(r|_{\Gamma_w}) = \{j - n - a_{\tau,j}\}_{j=1}^n.$$

In particular, r is Hodge-Tate regular.

(v) $\overline{F}^{\ker(\mathrm{ad}\,\bar{r})}$ does not contain $F(\zeta_\ell)$.
(vi) The group $\bar{r}(\mathrm{Gal}(\overline{F}/F(\zeta_\ell)))$ is big.
(vii) The representation $\bar{r}$ is irreducible and there is a conjugate self-dual, cohomological, cuspidal automorphic representation Π of $\mathrm{GL}_n(\mathbb{A}_F)$, of weight $\mathbf{a}$ and unramified above ℓ, and an isomorphism $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$, such that $\bar{r} \cong \bar{r}_{\ell,\iota}(\Pi)$.

Then r is automorphic of weight $\mathbf{a}$ and level prime to ℓ.

PROOF. Arguing as in **[Tay08**, Theorem 5.2], we may assume that F contains an imaginary quadratic field E with an embedding $\tau_E : E \hookrightarrow \overline{\mathbb{Q}}_\ell$ such that

$$\ell - 1 - n \geqslant a_{\tau,1} \geqslant \cdots \geqslant a_{\tau,n} \geqslant 0$$

for every $\tau : F \hookrightarrow \overline{\mathbb{Q}}_\ell$ extending τ_E. This will allow us to choose the set $\widetilde{S}_\ell$ (in the notation of Section 2.3) in such a way that the weights $a_{\tau,i}$ are all within the correct range for $\tau \in \widetilde{I}_\ell$. Let $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\simeq} \mathbb{C}$ and let Π be a conjugate self dual, cuspidal, cohomological automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$ of weight $\iota_*\mathbf{a}$, with Π_ℓ unramified, such that $\bar{r} \cong \bar{r}_{\ell,\iota}(\Pi)$. Let S_r denote the places of F not dividing ℓ at which r or Π is ramified. Since $\overline{F}^{\ker(\operatorname{ad}\bar{r})}$ does not contain $F(\zeta_\ell)$, we can choose a prime v_1 of F with the following properties.

- $v_1 \notin S_r$ and $v_1 \nmid \ell$.
- v_1 is unramified over a rational prime p, for which $[F(\zeta_p) : F] > n$.
- v_1 does not split completely in $F(\zeta_\ell)$.
- $\operatorname{ad}\bar{r}(\mathrm{Frob}_{v_1}) = 1$.

Choose a totally real field L^+/F^+ with the following properties.

- $2|[L^+ : \mathbb{Q}]$.
- L^+/F^+ is Galois and soluble.
- $L = L^+E$ is unramified over L^+ at every finite place.
- L is linearly disjoint from $\overline{F}^{\ker(\bar{r})}(\zeta_\ell)$ over F.
- ℓ is unramified in L.
- All primes of L above $S_r \cup \{v_1\}$ are split over L^+.
- v_1 and cv_1 split completely in L/F.
- Let Π_L denote the base change of Π to L. If v is a place of L above S_r, then
  - $Nv \equiv 1 (\operatorname{mod} \ell)$;
  - $\bar{r}(\mathrm{Gal}(\overline{L}_v/L_v)) = 1$;
  - $r|_{I_v}^{\mathrm{ss}} = 1$, and
  - $\Pi_{L,v}^{\mathrm{Iw}(v)} \neq 0$.

Since $[L^+ : \mathbb{Q}]$ is even, there exists a unitary group G in n variables attached to L/L^+ which is totally definite and such that G_v is quasi-split for every finite place v of L^+. Let $S_\ell(L^+)$ denote the set of primes of L^+ above ℓ, $S_r(L^+)$ the set of primes of L^+ lying above the restriction to F^+ of an element of S_r, and $S_a(L^+)$ the set of primes of L^+ above $v_1|_{F^+}$. Let $T(L^+) = S_\ell(L^+) \cup S_r(L^+) \cup S_a(L^+)$. It follows from Remarks 2.4 and 2.5 and Theorem 3.4 that $r|_{\mathrm{Gal}(\overline{F}/L)}$ is automorphic of weight $\mathbf{a}_L$ and level prime to ℓ, where $\mathbf{a}_L \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(L,\overline{\mathbb{Q}}_\ell)}$ is defined as $\mathbf{a}_{L,\tau} = \mathbf{a}_{\tau|_F}$. By Lemma 1.4 of **[BLGHT]** (note that the hypotheses there must say "$r^\vee \cong r^c \otimes \chi$" rather than "$r^\vee \cong r \otimes \chi$"), this implies that r itself is automorphic of weight $\mathbf{a}$ and level prime to ℓ.

□

We can also prove a modularity lifting theorem for totally real fields F^+. The proof goes exactly like that of Theorem 5.4 of **[Tay08]**, using Lemma 1.5 of **[BLGHT]** instead of Lemma 4.3.3 of **[CHT08]**.

THEOREM 4.2. *Let F^+ be a totally real field. Let $n \geqslant 1$ be an integer and $\ell > n$ be a prime number, unramified in F. Let*

$$r : \mathrm{Gal}(\overline{F}^+/F^+) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

be a continuous irreducible representation with the following properties. Let $\bar{r}$ denote the semisimplification of the reduction of r.

(i) $r^\vee \cong r(n-1) \otimes \chi$ for some character $\chi : \mathrm{Gal}(\overline{F}^+/F^+) \to \overline{\mathbb{Q}}_\ell^\times$ with $\chi(c_v)$ independent of $v|\infty$ (here c_v denotes a complex conjugation at v).

(ii) *r is unramified at all but finitely many primes.*
(iii) *For every place $v|\ell$ of F, $r|_{\Gamma_v}$ is crystalline.*
(iv) *There is an element $\mathbf{a} \in (\mathbb{Z}^{n,+})^{\mathrm{Hom}(F^+,\overline{\mathbb{Q}}_\ell)}$ such that*

- *for all $\tau \in \mathrm{Hom}(F^+, \overline{\mathbb{Q}}_\ell)$, we have either*
$$\ell - 1 - n \geqslant a_{\tau,1} \geqslant \cdots \geqslant a_{\tau,n} \geqslant 0$$
or
$$\ell - 1 - n \geqslant a_{\tau c,1} \geqslant \cdots \geqslant a_{\tau c,n} \geqslant 0;$$
- *for all $\tau \in \mathrm{Hom}(F^+, \overline{\mathbb{Q}}_\ell)$ and every $i = 1, \dots, n$,*
$$a_{\tau c,i} = -a_{\tau,n+1-i}.$$
- *for all $\tau \in \mathrm{Hom}(F^+, \overline{\mathbb{Q}}_\ell)$ giving rise to a prime $v|\ell$,*
$$\mathrm{HT}_\tau(r|_{\Gamma_v}) = \{j - n - a_{\tau,j}\}_{j=1}^n.$$
In particular, r is Hodge-Tate regular.

(v) *$(\overline{F}^+)^{\ker(\mathrm{ad}\,\bar{r})}$ does not contain $F^+(\zeta_\ell)$.*
(vi) *The group $\bar{r}(\mathrm{Gal}(\overline{F}^+/F^+(\zeta_\ell)))$ is big.*
(vii) *The representation $\bar{r}$ is irreducible and automorphic of weight $\mathbf{a}$.*

Then r is automorphic of weight $\mathbf{a}$ and level prime to ℓ.

CHAPTER 2

An algorithmic approach

Introduction

Modularity for elliptic curves over the rational numbers was one of the biggest achievements of the last century ([**Wil95, TW95, CDT99, BCDT01**]). The case of imaginary quadratic fields has been extensively investigated numerically by Cremona, starting with his Ph.D. thesis and the articles [**Cre84**], [**Cre92**] and [**CW94**]. More recently, some of his students extended the calculations to fields with higher class numbers. Their work focuses on the modular symbol method which relies on computing homology groups by tessellating the hyperbolic 3-space. This allows the computation of the Hecke eigenvalues of eigenforms. Doing a computer search, they furthermore exhibit candidates for matching elliptic curves by showing that the Euler factors of the L-function of the elliptic curve and that of the modular form are identical for all prime ideals up to a certain norm.

In this chapter we present an algorithm to determine whether the 2-adic Galois representations attached to an elliptic curve and a modular form f over F are isomorphic or not (whenever it makes sense to talk about the Galois representation attached to f). This algorithm allows to prove modularity for a variety of examples of elliptic curves, and it requires to have a list of the first Hecke eigenvalues of f; the number of elements needed varies on each case, but it is always finite. The algorithm is based on the Faltings-Serre method. For ℓ-adic Galois representations, this method enables one to prove isomorphy of the semisimplifications by comparing only a finite number of Euler factors.

This method has also been used by Taylor in [**Tay94**] (with $\ell = 2$) to prove the equality of the Euler factors of the elliptic curve over $\mathbb{Q}[\sqrt{-3}]$ of conductor $\left(\frac{17+\sqrt{-3}}{2}\right)$ (corresponding to the second case of our algorithm) for a set of density one primes, therefore (almost!) proving the modularity of the elliptic curve.

This chapter is organized as follows. In the first section we present the algorithm (which depends on the residual representations). In the second section we review the results of ℓ-adic representations attached to automorphic forms on imaginary quadratic fields. In the third section we explain the Falting-Serre method on Galois representations. In the fourth section we explain the algorithm and prove that it gives the right answer. In the last section, we show some examples and some GP code written for the examples.

1. Algorithm

Let F be an imaginary quadratic field, E be an elliptic curve over F and Π an automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ whose 2-adic Galois representations $r_2(E)$ and $r_2(\Pi)$ we want to compare (see Section 2). This algorithm answers whether these are isomorphic. Since these Galois representations come in compatible families, this also determines whether the ℓ-adic Galois representations are isomorphic or not for any prime ℓ. The algorithm depends on the residual image of the elliptic curve representation.

The input in all cases is: F, E, $\mathfrak{n}_E$ (the conductor of E), $\mathfrak{n}_\Pi$ (the level of Π) and $a_\mathfrak{p}(\Pi)$ for some prime ideals $\mathfrak{p}$ to be determined. By F_E we denote the field obtained from F by adding the coordinates of the 2-torsion points of E. For simplicity, we put $r_E = r_2(E)$ and $r_\Pi = r_2(\Pi)$. We denote by $\overline{r_E}$ and $\overline{r_\Pi}$ the semisimplifications of their reductions modulo 2. We denote by d_F the discriminant of F.

1.1. Residual image isomorphic to S_3.

(1) Let $\mathfrak{m}_F \subset \mathscr{O}_F$ be given by $\mathfrak{m}_F = \prod_{\mathfrak{p}|2\mathfrak{n}_E\mathfrak{n}_\Pi\overline{\mathfrak{n}_\Pi}d_F} \mathfrak{p}^{e(\mathfrak{p})}$ where

$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 6 \\ 2e(\mathfrak{p}|2)+1 & \text{if } \mathfrak{p} \mid 2 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$

Compute the ray class group $Cl(\mathscr{O}_F, \mathfrak{m}_F)$.

(2) Identify the character ψ corresponding to the unique quadratic extension of F contained in F_E on the computed basis.

(3) Extend $\{\psi\}$ to a basis $\{\psi, \chi_i\}_{i=1}^n$ of the quadratic characters of $Cl(\mathscr{O}_F, \mathfrak{m}_F)$. Compute prime ideals $\{\mathfrak{p}_j\}_{j=1}^{n'}$ of $\mathscr{O}_F$ with $\mathfrak{p}_j \nmid \mathfrak{m}_F$, and with inertial degree 3 in F_E such that

$$\left\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j))) \right\rangle_{j=1}^{n'} = (\mathbb{Z}/2\mathbb{Z})^n$$

(where we take any root of the logarithm and identify $\log(\pm 1)$ with $\mathbb{Z}/2\mathbb{Z}$).

(4) If $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_\mathfrak{p}))$ is odd for all prime ideals $\mathfrak{p}$ found in the last step, $\overline{r_\Pi}$ has image isomorphic to C_3 or to S_3 with the same intermediate quadratic field as $\overline{r_E}$. If not, end with output "the two representations are not isomorphic".

(5) Compute a basis $\{\chi_i\}_{i=1}^m$ of cubic characters of $Cl(\mathscr{O}_F, \mathfrak{m}_F)$ and a set of ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ such that $\psi(\mathfrak{p}_j) = -1$ or $\mathfrak{p}_j$ splits completely in F_E and

$$\left\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_m(\mathfrak{p}_j))) \right\rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m.$$

(6) If $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_\mathfrak{p}))$ is even for all prime ideals $\mathfrak{p}$ found in the last step, $\overline{r_\Pi}$ has S_3 image with the same intermediate quadratic field as $\overline{r_E}$. If not, end with output "the two representations are not isomorphic".

(7) Let $F'_E \subset F_E$ be the quadratic extension of F contained in F_E and let $\mathfrak{m}_{F'_E} \subset \mathscr{O}_{F'_E}$ be given by $\mathfrak{m}_{F'_E} = \prod_{\mathfrak{p}|2\mathfrak{n}_E\mathfrak{n}_\Pi\overline{\mathfrak{n}_\Pi}d_F} \mathfrak{p}^{e(\mathfrak{p})}$ where

$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 3 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$

Compute the ray class group $Cl(\mathscr{O}_{F'_E}, \mathfrak{m}_{F'_E})$.

(8) Identify the character ψ_E corresponding to the cubic extension F_E on the computed basis and extend it to a basis $\{\psi_E, \chi_i\}_{i=1}^m$ of order three characters of $Cl(\mathcal{O}_{F'_E}, \mathfrak{m}_{F'_E})$. Compute prime ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ of $\mathcal{O}_F$ such that $\psi_E(\mathfrak{p}_j) = 1$ and

$$\left\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j))) \right\rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$$

(where we take any identification of the cubic roots of unity with $\mathbb{Z}/3\mathbb{Z}$). If $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_j})) \equiv \mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_j})) \pmod 2$ for $1 \leqslant j \leqslant m'$, both residual representations are isomorphic. If not, end with output "the two representations are not isomorphic".

(9) Let $\mathfrak{m}_{F_E} \subset \mathcal{O}_{F_E}$ be defined by $\mathfrak{m}_{F_E} = \prod_{\mathfrak{q} | 2\mathfrak{n}_E \mathfrak{n}_\Pi \overline{\mathfrak{n}_\Pi} d_F} \mathfrak{q}^{e(\mathfrak{q})}$ where

$$e(\mathfrak{q}) = \begin{cases} 1 & \text{if } \mathfrak{q} \nmid 2 \\ 2e(\mathfrak{q}|2) + 1 & \text{if } \mathfrak{q} \mid 2. \end{cases}$$

Compute the ray class group $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_{F_E})$. Let $\{\mathfrak{a}_i\}_{i=1}^n$ be a basis for the even order elements of $Cl(\mathcal{O}_{F_E}, \mathfrak{m}_{F_E})$ and let $\{\chi_i\}_{i=1}^n$ be a basis for its quadratic characters (dual to the ray class group one computed).

(10) Compute the Galois group $\mathrm{Gal}(F_E/F)$.

(11) (Computing invariant subspaces) Let σ be an order 3 element of $\mathrm{Gal}(F_E/F)$ and solve the homogeneous system

$$\begin{pmatrix} \log(\chi_1(\mathfrak{a}_1\sigma(\mathfrak{a}_1))) & \ldots & \log(\chi_n(\mathfrak{a}_1\sigma(\mathfrak{a}_1))) \\ \vdots & & \vdots \\ \log(\chi_1(\mathfrak{a}_n\sigma(\mathfrak{a}_n))) & \ldots & \log(\chi_n(\mathfrak{a}_n\sigma(\mathfrak{a}_n))) \end{pmatrix}$$

Denote by V_σ the kernel.

(12) Take τ an order 2 element of $\mathrm{Gal}(F_E/F)$ and compute V_τ, the kernel of the same system for τ.

(13) Intersect V_σ with V_τ. Let $\{\chi_i\}_{i=1}^m$ be a basis of the intersection. This gives generators for the $S_3 \times C_2$ extensions.

(14) Compute a set of prime ideals $\{\mathfrak{p}_i\}_{i=1}^{m'}$ of $\mathcal{O}_F$ such that $\mathfrak{p}_i \nmid \mathfrak{m}_F$ and

$$\left\langle (\log(\chi_1(\tilde{\mathfrak{p}}_j)), \ldots, \log(\chi_n(\tilde{\mathfrak{p}}_j))) \right\rangle_{j=1}^{m'} = (\mathbb{Z}/2\mathbb{Z})^m,$$

where $\tilde{\mathfrak{p}}_i$ is any ideal of F_E above $\mathfrak{p}_i$.

(15) If $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_i}))$ for $1 \leqslant i \leqslant m$ then the two representations agree on order 6 elements, else end with output "the two representations are not isomorphic".

(16) For σ an order three element, solve the homogeneous system

$$\begin{pmatrix} \log(\chi_1(\mathfrak{a}_1\sigma(\mathfrak{a}_1)\sigma^2(\mathfrak{a}_1))) & \ldots & \log(\chi_n(\mathfrak{a}_1\sigma(\mathfrak{a}_1)\sigma^2(\mathfrak{a}_1))) \\ \vdots & & \vdots \\ \log(\chi_1(\mathfrak{a}_n\sigma(\mathfrak{a}_n))\sigma^2(\mathfrak{a}_n)) & \ldots & \log(\chi_n(\mathfrak{a}_n\sigma(\mathfrak{a}_n)\sigma^2(\mathfrak{a}_n))) \end{pmatrix}$$

Denote by W_σ such kernel.

(17) Intersect W_σ with V_τ. Let $\{\chi_i\}_{i=1}^{t}$ be a basis of such subspace. This characters give all the S_4 extensions.

(18) Compute a set of prime ideals $\{\mathfrak{p}_i\}_{i=1}^{t'}$ of $\mathcal{O}_F$ such that $\mathfrak{p}_i \nmid \mathfrak{m}_F$ and

$$\left\langle (\log(\chi_1(\tilde{\mathfrak{p}}_j)),\ldots,\log(\chi_n(\tilde{\mathfrak{p}}_j))),\ldots,(\log(\chi_1(\sigma^2(\tilde{\mathfrak{p}}_j))),\ldots,\log(\chi_n(\sigma^2(\tilde{\mathfrak{p}}_j))))\right\rangle_{j=1}^{t'}$$

equals $(\mathbb{Z}/2\mathbb{Z})^t$, where $\tilde{\mathfrak{p}}_i$ is any ideal of F_E above $\mathfrak{p}_i$.

(19) If $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_i}))$ for all $1 \leqslant i \leqslant n$ output "$r_f \cong r_{\mathcal{E}}$". Otherwise, output "the two representations are not isomorphic".

1.2. Residual image trivial or isomorphic to C_2.

(1) Choose prime ideals $\mathfrak{p}_i$, $i = 1,2$, such that if $\alpha_{\mathfrak{p}_i}$ and $\beta_{\mathfrak{p}_i}$ denote the roots of the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{p}_i}$, then $\alpha_{\overline{\mathfrak{p}}_i} + \beta_{\overline{\mathfrak{p}}_i} \neq 0$ and 2 has no inertial degree in the extension $\mathbb{Q}[\alpha_{\mathfrak{p}_i}]$. If $\mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_i})) \neq \mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ for $i = 1$ or 2, end with output "the two representations are not isomorphic".

(2) Let $\mathfrak{m}_F \subset \mathcal{O}_F$ be given by $\mathfrak{m}_F = \prod_{\mathfrak{p}|2\mathfrak{n}_E\mathfrak{n}_\Pi\overline{\mathfrak{n}_\Pi}d_F} \mathfrak{p}^{e(\mathfrak{p})}$ where

$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 6 \\ 2e(\mathfrak{p}|2)+1 & \text{if } \mathfrak{p} \mid 2 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$

Compute the ray class group $Cl(\mathcal{O}_F, \mathfrak{m}_F)$.

(3) For each subgroup of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$ of index 1 or 2, take the corresponding quadratic (or trivial) extension L. In L, take the modulus $\mathfrak{m}_L = \prod_{\mathfrak{p}|2\mathfrak{n}_E\mathfrak{n}_\Pi\overline{\mathfrak{n}_\Pi}d_F} \mathfrak{p}^{e(\mathfrak{p})}$, where

$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 3 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$

and compute the ray class group $Cl(\mathcal{O}_L, \mathfrak{m}_L)$.

(4) Compute a set of generators $\{\chi_j\}_{j=1}^{n}$ for the cubic characters of $Cl(\mathcal{O}_L, \mathfrak{m}_L)$, and find prime ideals $\{\mathfrak{q}_j\}_{j=1}^{n'}$ of $\mathcal{O}_L$, with $\mathfrak{q}_j \nmid \mathfrak{m}_L$ and such that

$$\langle (\log(\chi_1(\mathfrak{q}_j)),\ldots,\log(\chi_n(\mathfrak{q}_j)))\rangle_{j=1}^{n'} = (\mathbb{Z}/3\mathbb{Z})^n.$$

(5) Consider the collection $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_m\}$ of all prime ideals of $\mathcal{O}_F$ which are below the prime ideals found in step (4).

(6) If $\mathrm{Tr}(\overline{r_\Pi}(\mathrm{Frob}_{\mathfrak{p}_i})) \equiv 0 \pmod 2$ for all prime ideals $\mathfrak{p}$ found in the last step, then the image of $\overline{r_\Pi}$ is either trivial or isomorphic to C_2. Otherwise, output "the two representations are not isomorphic".

(7) Compute a basis $\{\chi_i\}_{i=1}^{n}$ of quadratic characters of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$.

(8) Compute a set of prime ideals $\{\mathfrak{p}_i \subset \mathcal{O}_F \,:\, \mathfrak{p}_i \nmid \mathfrak{m}_F\}_{i=1}^{2^n-1}$ such that

$$\{(\log(\chi_1(\mathfrak{p}_i)),\ldots,\log(\chi_n(\mathfrak{p}_i))\}_{i=1}^{2^n-1} = (\mathbb{Z}/2\mathbb{Z})^n\backslash\{0\}$$

(9) If $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_i}))$ for $i = 1, \ldots, 2^n - 1$, then $r_E^{ss} \cong r_\Pi^{ss}$. Otherwise, output "the two representations are not isomorphic".

REMARK 1.1. The algorithm can be slightly improved. In step (8), instead of aiming at the whole C_2^r, we can stop when we reach a *non-cubic* set.

DEFINITION. Let V be a finite dimensional vector space. A subset T of V is called *non-cubic* if each homogeneous polynomial on V of degree 3 that is zero on T, is zero on V.

In particular, the whole space V is non-cubic. The following result is useful for identifying non-cubic subsets of $(\mathbb{Z}/2\mathbb{Z})$-vector spaces.

PROPOSITION 1.2. *Let V be a vector space over $\mathbb{Z}/2\mathbb{Z}$. Then a function $f : V \to \mathbb{Z}/2\mathbb{Z}$ is represented by a homogeneous polynomial of degree* 3 *if and only if* $\sum_{I\subset\{0,1,2,3\}} f(\sum_{i\in I} v_i) = 0$ *for every subset* $\{v_0, v_1, v_2, v_3\} \subset V$.

PROOF. See **[Liv87]**. ☐

1.3. Residual image isomorphic to C_3.

(1) Choose prime ideals $\mathfrak{p}_i$, $i = 1, 2$, such that if $\alpha_{\mathfrak{p}_i}$ and $\beta_{\mathfrak{p}_i}$ denote the roots of the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{p}_i}$, then $\alpha_{\overline{\mathfrak{p}}_i} + \beta_{\overline{\mathfrak{p}}_i} \neq 0$ and 2 has no inertial degree on the extension $\mathbb{Q}[\alpha_{\mathfrak{p}_i}]$. If $\mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_i})) \neq \mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_i}))$ for $i = 1$ or 2, end with output "the two representations are not isomorphic".

(2) Let $\mathfrak{m}_F \subset \mathcal{O}_F$ be given by $\mathfrak{m}_F = \prod_{\mathfrak{p}|2\mathfrak{n}_E\mathfrak{n}_\Pi\overline{\mathfrak{n}_\Pi}d_F} \mathfrak{p}^{e(\mathfrak{p})}$, where

$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 6 \\ 2e(\mathfrak{p}|2) + 1 & \text{if } \mathfrak{p} \mid 2 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$

Compute the ray class group $Cl(\mathcal{O}_F, \mathfrak{m}_F)$.

(3) Identify the character ψ_E corresponding to the cubic Galois extension F_E on the computed basis.

(4) Find a basis $\{\chi_i\}_{i=1}^n$ of the quadratic characters of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$. Compute prime ideals $\{\mathfrak{p}_j\}_{j=1}^{n'}$ of $\mathcal{O}_F$ such that $\mathfrak{p}_j \nmid \mathfrak{m}_F$, $\psi(\mathfrak{p}_j) \neq 1$ and

$$\left\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j))) \right\rangle_{j=1}^{n'} = (\mathbb{Z}/2\mathbb{Z})^n$$

(where we take any root of the logarithm and identify $\log(\pm 1)$ with $\mathbb{Z}/2\mathbb{Z}$).

(5) If $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_\mathfrak{p}))$ is odd for all prime ideals $\mathfrak{p}$ found in the last step, then the image of $\overline{r_\Pi}$ is isomorphic to C_3. Otherwise, end with output "the two representations are not isomorphic".

(6) Extend $\{\psi_E\}$ to a basis $\{\psi_E, \chi_i\}_{i=1}^m$ of order three characters of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$. Compute prime ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ of $\mathcal{O}_F$ such that $\psi_E(\mathfrak{p}_j) = 1$ and

$$\left\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j))) \right\rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$$

(where we take any root of the logarithm and identify log of the cubic roots of unity with $\mathbb{Z}/3\mathbb{Z}$). If $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_j})) \equiv \mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_j})) \pmod 2$ for $1 \leqslant j \leqslant m'$, then $\overline{r_E} \cong \overline{r_\Pi}$. Otherwise, end with output "the two representations are not isomorphic".

(7) Apply the previous case, steps (7) to (10), with F replaced by F_E.

2. Galois representations attached to elliptic curves and modular forms

Let F be an imaginary quadratic field. We want to consider two-dimensional, irreducible, ℓ-adic representations of the group Γ_F.

Let E be an elliptic curve over F. The Tate module $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2 with a continuous linear action of Γ_F, giving rise to an ℓ-adic representation

$$r_\ell(E) : \Gamma_F \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

In order to make sure that the Galois representation $r_\ell(E)$ is absolutely irreducible we will assume that E does not have complex multiplication. The ramification locus of the representation $r_\ell(E)$ consists of those primes of F dividing ℓ together with the set of primes of bad reduction of E. The family of Galois representations $\{r_\ell(E)\}$ is a compatible family and has conductor equal to the conductor of the elliptic curve E.

On the other hand, Harris, Soudry and Taylor ([**HST93**]), Taylor ([**Tay94**]) and Berger-Harcos ([**BH07**]) have proved that one can attach compatible families of two-dimensional Galois representations to any cohomological cuspidal automorphic representation Π of $\mathrm{GL}_2(\mathbb{A}_F)$ (see * for the definition of cohomological), assuming that it has unitary central character ω with $\omega = \omega^c$, where c is the non-trivial Galois automorphism of $F/\mathbb{Q}$. This is equivalent to saying that the central character is the restriction of a character of $\Gamma_\mathbb{Q}$. As in the case of classical modular forms, "to be attached" should mean that there is a correspondence between the ramification loci of Π and that of the representation $r_\ell(\Pi)$, and that at the other places $\mathfrak{p}$, the characteristic polynomial of $r_\ell(\Pi)(\mathrm{Frob}_\mathfrak{p})$ agrees with the Hecke polynomial of Π at $\mathfrak{p}$. However, since the method for constructing these Galois representations depends on using a theta lift to link with automorphic forms on $\mathrm{GSp}_4(\mathbb{A}_\mathbb{Q})$, it can not be excluded that the representation $r_\ell(\Pi)$ also ramifies at the primes that ramify in $F/\mathbb{Q}$. The precise statement of the result, valid only under the assumption $\omega = \omega^c$, is the following (cf. [**Tay94**], [**HST93**] and [**BH07**]):

THEOREM 2.1. *Let S be the set of places in F consisting of those dividing ℓ and those where either $F/\mathbb{Q}$, Π or Π^c ramify. Then there exists an irreducible continuous representation:*

$$r_\ell(\Pi) : \Gamma_F \to \mathrm{GL}_2(\bar{\mathbb{Q}}_\ell)$$

such that if $\mathfrak{p}$ is a prime of F which is not in S, then $r_\ell(\Pi)$ is unramified at $\mathfrak{p}$ and the characteristic polynomial of $r_\ell(\Pi)(\mathrm{Frob}_\mathfrak{p})$ agrees with the Hecke polynomial of Π at $\mathfrak{p}$

REMARK 2.2. If for some prime $\mathfrak{p}$, ramified in $F/\mathbb{Q}$, we happen to know that $r_\ell(\Pi)$ is unramified at $\mathfrak{p}$, the above theorem does not imply that the characteristic polynomial of $r_\ell(\Pi)(\mathrm{Frob}_\mathfrak{p})$ agrees with the Hecke polynomial of Π at $\mathfrak{p}$, though it is expected that these two values should agree. It is also expected that there is a conductor for the family $\{r_\ell(\Pi)\}$, that is to say, that the conductor should be independent of ℓ as in the case of elliptic curves. The value of this conductor should also agree with the level of Π.

REMARK 2.3. Since the families of Galois representations attached to an elliptic curve E over F and to a cuspidal automorphic representation Π as above are both compatible families, if $r_\ell(E) \cong r_\ell(\Pi)$ for some prime ℓ, then the same holds for every prime ℓ.

From now on, we will assume that the field generated by the traces of Frobenius elements is the rational field $\mathbb{Q}$, since these are the newforms corresponding to elliptic curves.

REMARK 2.4. By standard arguments, $r_\ell(\Pi)$ takes values in $\mathrm{GL}_2(\mathscr{O}_L)$, where $\mathscr{O}_L$ is the ring of integers of a finite extension L of $\mathbb{Q}_\ell$. In fact, we can take L with $[L : \mathbb{Q}_\ell] \leqslant 4$. Furthermore, let v_i, $i = 1,2$ be two unramified paces of F and let α_i, β_i be the roots of the characteristic polynomial of Frob_{v_i}. If $\alpha_{v_i} \neq \beta_{v_i}$ and, in the case v_i is split, $\alpha_{\overline{v_i}} + \beta_{\overline{v_i}} \neq 0$, then we can take L to be the completion at any prime above ℓ of the field $\mathbb{Q}[\alpha_{v_1}, \alpha_{v_2}]$ (see Corollary 1 of **[Tay94]**).

3. Faltings-Serre method

3.1. First case: the residual image is absolutely irreducible. In this section we review the Faltings-Serre (**[Ser85]**) method by stating the main ideas of **[Sch06]** (Section 5) in our particular case. Take $\ell = 2$ and let

$$r_i : \Gamma_F \to \mathrm{GL}_2(\mathbb{Z}_2)$$

be representations for $i = 1,2$ such that they satisfy:

- They have the same determinant.
- They are unramified outside a finite set S.
- The mod 2 reductions are absolutely irreducible and isomorphic.
- There exists a prime $\mathfrak{p}$ such that $\mathrm{Tr}(r_1(\mathrm{Frob}_\mathfrak{p})) \neq \mathrm{Tr}(r_2(\mathrm{Frob}_\mathfrak{p}))$.

We want to give a finite set of candidates for $\mathfrak{p}$. Choose the maximal r such that $\mathrm{Tr}(r_1) \equiv \mathrm{Tr}(r_2) \pmod{2^r}$, and consider the non-trivial map $\phi : \Gamma_F \to \mathbb{F}_2$ given by

$$\phi(\sigma) \equiv \frac{\mathrm{Tr}(r_1(\sigma)) - \mathrm{Tr}(r_2(\sigma))}{2^r} \pmod{2}.$$

Since the mod 2 residual representations $\overline{r_1}$ and $\overline{r_2}$ are absolutely irreducible and their images are isomorphic, we can assume that $\overline{r_1} = \overline{r_2}$.

Since $\mathrm{Tr}\, r_1 \equiv \mathrm{Tr}\, r_2 \pmod{2^r}$, given $\sigma \in \Gamma_F$, there exists $\mu(\sigma) \in M_2(\mathbb{Z}_2)$ such that

$$r_1(\sigma) = (1 + 2^r \mu(\sigma)) r_2(\sigma).$$

Then,

$$\phi(\sigma) = \frac{\mathrm{Tr}(r_1(\sigma)) - \mathrm{Tr}(r_2(\sigma))}{2^r} = \mathrm{Tr}(\mu(\sigma) r_2(\sigma)) \equiv \mathrm{Tr}(\mu(\sigma)\overline{r}_1(\sigma)) \pmod{2}. \tag{3.1.1}$$

Consider the map $\varphi : \Gamma_F \to M_2(\mathbb{F}_2) \rtimes \operatorname{im}(\overline{r_1})$ given by

$$\varphi(\sigma) = (\mu(\sigma), \bar{r}_1(\sigma)) \pmod 2.$$

An easy computation shows that

$$\mu(\sigma\tau) \equiv \mu(\sigma) + \bar{r}_1(\sigma)^{-1}\mu(\tau)\bar{r}_1(\sigma) \pmod 2,$$

which implies that φ is a group morphism. Furthermore, since $\ker(\phi)$ contains the group $\{\sigma \in \Gamma_F \ : \ \mu(\sigma) \equiv 0 \pmod 2\} \rtimes \{1\}$, ϕ factors through $M_2(\mathbb{F}_2) \rtimes \operatorname{im}(\overline{r_1})$. We have the diagram

$$\begin{tikzcd} \Gamma_F \arrow[rr, "\phi"] \arrow[dr, "\varphi"'] & & \mathbb{F}_2 \\ & M_2(\mathbb{F}_2) \rtimes \operatorname{im}(\overline{r_1}) \arrow[ur, "\phi"'] & \end{tikzcd}$$

By (3.1.1), ϕ is defined on $M_2(\mathbb{F}_2) \rtimes \operatorname{im}(\tilde{r_1})$ by $\phi(A, C) = \operatorname{Tr}(AC)$. Let $\overline{\mu}$ denote the composition of μ with reduction modulo 2. Since

$$\det(r_1(\sigma)) \equiv (1 + 2^r \operatorname{Tr}(\mu(\sigma))) \det(r_2(\sigma)) \pmod{2^{r+1}},$$

the condition $\det(r_1) = \det(r_2)$ implies that $\operatorname{im}(\overline{\mu}) \subset M_2^0(\mathbb{F}_2) := \{M \in M_2(\mathbb{F}_2) \ : \ \operatorname{Tr}(M) \equiv 0 \pmod 2\}$, hence it has order at most 2^3. In our case, $\operatorname{im}(\bar{r}_i) = S_3$.

LEMMA 3.1. $M_2^0(\mathbb{F}_2) \rtimes S_3 \simeq S_4 \times C_2$.

This can be proved in different ways, we give an explicit isomorphism for latter considerations. Take the isomorphism between $\mathrm{GL}_2(\mathbb{F}_2)$ and S_3 given by

$$\begin{aligned} (12) &\mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \\ (13) &\mapsto \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right). \end{aligned}$$

Take $\left\{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$ as a basis for $M_2^0(\mathbb{F}_2)$. It is clear that the action of S_3 on the last element is trivial. If we denote v_1, v_2 the first two elements of the basis and v_3 their sum, the action of $\sigma \in S_3$ on the Klein group $C_2 \times C_2$ (spanned by v_1 and v_2) is $\sigma(v_i) = v_{\sigma(i)}$. Since $S_4 \simeq S_3 \ltimes (C_2 \times C_2)$ with the same action as described above we get the desired isomorphism.

Clearly the elements of $S_3 \times \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\{1\} \times M_2^0(\mathbb{F}_2)$ and $\{\sigma \in S_3 \ : \ \sigma^2 = 1\} \times \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ go to 0 by ϕ. It can be seen that all the other elements have non-trivial image (which correspond to the elements of order 4 or 6 in $S_4 \times C_2$). If we denote by K the fixed field of $\ker(\bar{r}_1)$, we need to compute all possible extensions $\tilde{K}$ of K which are Galois over F, unramified outside S and with Galois group over F isomorphic to a subgroup of $S_4 \times C_2$. For each $\tilde{K}$, take a prime ideal $\mathfrak{p}_{\tilde{K}} \subset F$ with inertial degree 4 or 6 on $\tilde{K}$. Then $\{\mathfrak{p}_{\tilde{K}}\}$ has the desired properties.

REMARK 3.2. In the proof given above one starts with a mod ℓ^r congruence between the traces of r_1 and r_2 and uses the fact that this implies that the two mod ℓ^r representations are isomorphic. This result is proved in **[Ser95]** (Theorem 1) but only with the assumption that the residual mod ℓ representations are absolutely irreducible. In fact, it is false in the residually reducible case, and this is one of the reasons why the above method does not extend to the case of residual image cyclic of order 3. When the residual representations are reducible there are counter-examples to this claim even assuming that they are semi-simple. We thank Professor J.-P. Serre for pointing out the following counter-example to us: take $\ell = 2$ and consider two characters χ and χ' defined $\bmod 2^r$ such that they agree $\bmod 2^{r-1}$ but not $\bmod 2^r$. Then $\chi \oplus \chi$ and $\chi' \oplus \chi'$ are two-dimensional Galois representations defined $\bmod 2^r$ having the same trace but they are not isomorphic.

3.2. Second case: the image is a 2-group. This case was treated in **[Liv87]**, where the author proves the following result.

THEOREM 3.3. *Let F be an imaginary quadratic field, S a finite set of primes of F and L a finite extension of $\mathbb{Q}_2$. Denote by F_S the compositum of all quadratic extensions of F unramified outside S and by λ_L the maximal ideal of $\mathcal{O}_L$. Suppose $r_1, r_2 : \Gamma_F \to \mathrm{GL}_2(L)$ are continuous representations, unramified outside S, satisfying:*

1. $\mathrm{Tr}(r_1) \equiv \mathrm{Tr}(r_2) \equiv 0 \pmod{\lambda_L}$ *and* $\det(r_1) \equiv \det(r_2) \pmod{\lambda_L}$.
2. *There exists a set T of primes of F, disjoint from S, for which*
   - *(i) The image of the set $\{\mathrm{Frob}_t\}$ in the $(\mathbb{Z}/2\mathbb{Z})$-vector space $\mathrm{Gal}(F_S/F)$ is non-cubic.*
   - *(ii)* $\mathrm{Tr}(r_1(\mathrm{Frob}_t)) = \mathrm{Tr}(r_2(\mathrm{Frob}_t))$ *and* $\det(r_1(\mathrm{Frob}_t)) = \det(r_2(\mathrm{Frob}_t))$ *for all $t \in T$.*

Then r_1 and r_2 have isomorphic semi-simplifications.

PROOF. See **[Liv87]**. □

3.3. Third case: the image is cyclic of order 3. This is a mix of the previous two cases. Let L be a finite extension of $\mathbb{Q}_2$ with residue field isomorphic to $\mathbb{F}_2$. Suppose $r_1, r_2 : \Gamma_F \to \mathrm{GL}_2(L)$ are continuous representations such that the residual representations are isomorphic and have image a cyclic group of order 3. Let F_r be the fixed field of the residual representations kernels. If we restrict the two representations to $\mathrm{Gal}(\bar{F}/F_r)$, we get:

$$r_1, r_2 : \mathrm{Gal}(\bar{F}/F_r) \to \mathrm{GL}_2(L),$$

whose residual representations have trivial image. Hence we are in the 2-group case for the field F_r and Livne's Theorem 3.3 applies.

4. Proof of the Algorithm

Before giving a proof for each case we make some general considerations. Recall that we note $r_E = r_2(E)$ and $r_\Pi = r_2(\Pi)$. The image of $\overline{r_E}$ is isomorphic to the Galois group $\mathrm{Gal}(F_E/F)$. If $E(F)$ has a 2-torsion point, the image of $\overline{r_E}$ is a 2-group. If not, assume (via a change of variables) that the elliptic curve has equation

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

and denote by α, β, γ the roots of $x^3 + a_2x^2 + a_4x + a_6$. Using elementary Galois theory it can be seen that $F_E = F[\alpha - \beta]$. Furthermore, using elementary symmetric functions, it can be seen that $\alpha - \beta$ is a root of the polynomial

$$x^6 + x^4(6a_4 - 2a_2^2) + x^2(a_2^4 - 6a_2^2a_4 + 9a_4^2) + 4a_6a_2^3 - 18a_6a_4a_2 + 4a_4^3 - a_4^2a_2^2 + 27a_6^2.$$

If this polynomial is irreducible over F, the image of $\overline{r_E}$ is isomorphic to S_3 while if it is reducible, the image is isomorphic to C_3.

Note that under the isomorphism between S_3 and $\mathrm{GL}_2(\mathbb{F}_2)$ given in the previous section, the order 1 or 2 elements of S_3 have even trace while the order 3 ones have odd trace.

In the case where the image is not absolutely irreducible, we need to prove that the image lies (after conjugation) in an extension L of $\mathbb{Q}_2$ with residual field $\mathbb{F}_2$.

THEOREM 4.1. *If E has no complex multiplication, then we can choose split primes of F, $\mathfrak{p}_i$, $i = 1, 2$ such that if $\alpha_{\mathfrak{p}_i}, \beta_{\mathfrak{p}_i}$ denote the roots of the characteristic polynomial of* $\mathrm{Frob}_{\mathfrak{p}_i}$, *then $\alpha_{\mathfrak{p}_i} \neq \beta_{\mathfrak{p}_i}$, the field* $\mathbb{Q}[\alpha_{\mathfrak{p}_i}]$ *has inertial degree* 1 *at* 2 *and $\alpha_{\bar{\mathfrak{p}}_i} + \beta_{\bar{\mathfrak{p}}_i} \neq 0$. If* $\mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(r_\Pi(\mathfrak{p}_i))$ *for such primes, by Taylor's argument (see Remark 2.4),* $\mathrm{im}(\overline{r_\Pi}) \subset \mathrm{GL}_2(\mathbb{F}_2)$.

PROOF. Since E has no complex multiplication, if K is any quadratic extension of $\mathbb{Q}_2$, the set of primes $\mathfrak{p}$ such that $\mathbb{Q}_2[\alpha_\mathfrak{p}] = K$ has positive density (see for example Exercise 3, page IV-14 of **[Ser68]**). Also, the set of primes $\mathfrak{p}$ such that $\alpha_\mathfrak{p} + \beta_\mathfrak{p} = 0$ has density zero (since E has no complex multiplication, see **[Ser66]**), so we can find primes $\mathfrak{p}$ such that $\mathbb{Q}_2[\alpha_\mathfrak{p}] = K$ and $\alpha_{\bar{\mathfrak{p}}} + \beta_{\bar{\mathfrak{p}}} \neq 0$. The fields K_1 and K_2 obtained by adding the roots of the polynomials $x^2 + 14$ and $x^2 + 6$ to $\mathbb{Q}_2$ (whose roots in $\bar{\mathbb{Q}}_2$ are different) are two ramified extensions of $\mathbb{Q}_2$. Their composition is a degree 4 field extension (since the prime 2 is totally ramified in the composition of these extensions over $\mathbb{Q}$). Since the set of primes inert in F have density zero, we can choose prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ such that $\mathbb{Q}_2[\alpha_{\mathfrak{p}_1}]$ and $\mathbb{Q}_2[\alpha_{\mathfrak{p}_2}]$ are isomorphic to K_1 and K_2 respectively. □

Actually we search for the first two primes such that if $\alpha_{\mathfrak{p}_i}$ and $\beta_{\mathfrak{p}_i}$ denote the roots of the characteristic polynomial of their Frobenius automorphisms, $\alpha_{\bar{\mathfrak{p}}_i} + \beta_{\bar{\mathfrak{p}}_i} \neq 0$ and in the extension $\mathbb{Q}[\alpha_{\mathfrak{p}_i}]$, 2 has no inertial degree.

The first step of the algorithm is to prove that the residual representations are indeed isomorphic so as to apply Faltings-Serre method. In doing this we need to compute all extensions of a fixed degree (2 or 3 in our case) with prescribed ramification. Since we deal with abelian extensions, we can use class field theory.

THEOREM 4.2. *If L/F is an abelian extension unramified outside the set of places $\{\mathfrak{p}_i\}_{i=1}^n$ then there exists a modulus $\mathfrak{m} = \prod_{i=1}^n \mathfrak{p}_i^{e(\mathfrak{p}_i)}$ such that* $\mathrm{Gal}(L/F)$ *corresponds to a subgroup of the ray class group $Cl(\mathscr{O}_F, \mathfrak{m})$.*

Since we are interested in the case F an imaginary quadratic field, all the ramified places of L/F are finite ones, hence $\mathfrak{m}$ is an ideal in $\mathscr{O}_F$. A bound for $e(\mathfrak{p})$ is given by the following result.

PROPOSITION 4.3. *Let L/F be an abelian extension of prime degree p. If $\mathfrak{p}$ ramifies in L/F, then*

$$\begin{cases} e(\mathfrak{p}) = 1 & \text{if } \mathfrak{p} \nmid p \\ 2 \leqslant e(\mathfrak{p}) \leqslant \left\lfloor \frac{pe(\mathfrak{p}|p)}{p-1} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid p. \end{cases}$$

PROOF. See **[Coh00]** Proposition 3.3.21 and Proposition 3.3.22. □

To distinguish representations, given a character ψ of a ray class field we need to find a prime ideal $\mathfrak{p}$ with $\psi(\mathfrak{p}) \neq 1$. Let ψ be a character of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$ of prime order p. Take any branch of the logarithm over $\mathbb{C}$ and identify $\log(\{\zeta_p^i\})$ with $\mathbb{Z}/p\mathbb{Z}$ in any way (where ζ_p denotes a primitive p-th root of unity).

PROPOSITION 4.4. *Let F be a number field, $\mathfrak{m}_F$ a modulus and $Cl(\mathcal{O}_F, \mathfrak{m}_F)$ the ray class group for $\mathfrak{m}_F$. Let $\{\psi_i\}_{i=1}^n$ be a basis of order p characters of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$ and $\{\mathfrak{p}_j\}_{j=1}^{n'}$ be prime ideals of $\mathcal{O}_F$ such that*

$$\left\langle \log(\psi_1(\mathfrak{p}_j)), \ldots, \log(\psi_n(\mathfrak{p}_j)) \right\rangle_{j=1}^{n'} = (\mathbb{Z}/p\mathbb{Z})^n.$$

Then for every non trivial character ψ of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$ of order p, $\psi(\mathfrak{p}_j) \neq 1$ for some $1 \leqslant j \leqslant n'$.

PROOF. Suppose that $\psi(\mathfrak{p}_j) = 1$ for $1 \leqslant j \leqslant n'$. Since $\{\psi_i\}_{i=1}^n$ is a basis, there exists exponents ε_i such that

$$\psi = \prod_{i=1}^{n} \psi_i^{\varepsilon_i}$$

Taking logarithm and evaluating at $\mathfrak{p}_j$ we see that $(\varepsilon_1, \ldots \varepsilon_n)$ is a solution of the homogeneous system

$$\begin{pmatrix} \log(\psi_1(\mathfrak{p}_1)) & \ldots & \log(\psi_n(\mathfrak{p}_1)) \\ \vdots & & \vdots \\ \log(\psi_1(\mathfrak{p}_{n'})) & \ldots & \log(\psi_n(\mathfrak{p}_{n'})) \end{pmatrix}.$$

Since $\left\{(\log(\psi_1(\mathfrak{p}_j)), \ldots, \log(\psi_n(\mathfrak{p}_j)))\right\}_{j=1}^{n'}$ span $(\mathbb{Z}/p\mathbb{Z})^n$, the matrix has maximal rank, hence $\varepsilon_i = 0$ and ψ is the trivial character. □

REMARK 4.5. A set of prime ideals satisfying the conditions of the previous Proposition always exists by Tchebotarev's density theorem. What we do in practice is to enlarge the matrix

$$\begin{pmatrix} \log(\psi_1(\mathfrak{p}_1)) & \ldots & \log(\psi_n(\mathfrak{p}_1)) \\ \vdots & & \vdots \\ \log(\psi_1(\mathfrak{p}_m)) & \ldots & \log(\psi_n(\mathfrak{p}_m)) \end{pmatrix},$$

with enough prime ideals of F until it has rank n.

4.1. Residual image isomorphic to S_3.

REMARK 4.6. If the residual representation is absolutely irreducible, we can apply a descent result (see Corollaire 5 in **[Ser95]**,which can be applied because the Brauer group of a finite field is trivial) and conclude that since the traces are all in $\mathbb{F}_2$ the representation can be defined (up to isomorphism) as a representation with values on a two-dimensional $\mathbb{F}_2$-vector space. Thus, the image can be assumed to be contained in $\mathrm{GL}_2(\mathbb{F}_2)$ and because of the absolute irreducibility assumption we conclude that the image has to be isomorphic to S_3.

Furthermore, we have the following result,

THEOREM 4.7. *Assume that the traces of Frobenius elements of a 2-dimensional ℓ-adic Galois representation are all in $\mathbb{Q}_\ell$ and that the residual representation is absolutely irreducible, then the field L can be taken to be $\mathbb{Q}_\ell$.*

PROOF. This follows from the same argument as the previous Remark. See also Corollary of **[CSS97]**, page 256. $\square$

REMARK 4.8. Since all our traces lie in $\mathbb{Q}_2$, once we prove that the residual representation of r_Π has image strictly greater than C_3 we automatically know that it can be defined on $\mathrm{GL}_2(\mathbb{Z}_2)$.

We have the 2-adic Galois representations r_E and r_Π and we want to prove that they are isomorphic. We start by proving that the reduced representations are isomorphic. The first step is to prove that if F_Π denotes the fixed field of the kernel of r_Π, then it contains no quadratic extension of F or it contains F'_E, the quadratic extension of F contained in F_E.

We compute all quadratic extensions of F using Class Field theory and Proposition 4.3. Let ψ be the quadratic character of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$ associated to F'_E. We extend $\{\psi\}$ to a basis $\{\psi, \chi_i\}_{i=1}^n$ of the quadratic characters of $Cl(\mathcal{O}_F, \mathfrak{m}_F)$ and find a set of unramified prime ideals $\{\mathfrak{p}_j\}_{j=1}^{n'}$ with inertial degree 3 on F_E and such that $\left\langle(\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j)))\right\rangle_{j=1}^{n'} = (\mathbb{Z}/2\mathbb{Z})^n$. Since an ideal with inertial degree 3 on F_E splits on F'_E, $\psi(\mathfrak{p}_i) = 1$ for all $1 \leqslant i \leqslant n'$.

If χ is a quadratic character corresponding to a subfield of F_Π, $\chi = \psi^\varepsilon \varkappa$, where $\varkappa = \prod_{i=1}^n \chi_i^{\varepsilon_i}$. If $\varkappa = 1$, then $\chi = \psi$ or trivial and we are done. Otherwise, by Proposition 4.4, there exists an index i_0 such that $\varkappa(\mathfrak{p}_{i_0}) \neq 1$. Furthermore, since $\psi(\mathfrak{p}_{i_0}) = 1$, $\chi(\mathfrak{p}_{i_0}) \neq 1$. Hence $\mathrm{Tr}(\overline{r_\Pi}(\mathfrak{p}_{i_0})) \equiv 0 \pmod 2$ and $\mathrm{Tr}(\overline{r_E}(\mathfrak{p}_{i_0})) \equiv 1 \pmod 2$ which implies that the residual representations are not isomorphic. This is done in steps $(1) - (4)$.

REMARK 4.9. Let $P(X)$ denote the degree 3 polynomial in $F[X]$ whose roots are the x-coordinates of the points of order 2 of E. The fact that the splitting field of $P(X)$ is an S_3 extension allows us to compute how primes decompose in F'_E knowing how they decompose in the cubic extension F_P of F obtained by adjoining any root of $P(X)$.

The factorization as well as the values of $\psi(\mathfrak{p})$ are given by the next table:

$\mathfrak{p}\mathscr{O}_{F_P}$	$\mathfrak{p}\mathscr{O}_{F'_E}$	$\mathfrak{p}\mathscr{O}_{F_E}$	$\psi(\mathfrak{p})$
$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2$	$\mathfrak{t}_1\dots\mathfrak{t}_6$	1
$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{t}_1\mathfrak{t}_2\mathfrak{t}_3$	-1
$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	$\mathfrak{t}_1\mathfrak{t}_2$	1

PROOF. The last two cases are the easy ones: if $\mathfrak{p}$ is inert in $\mathscr{O}_{F_P}$, the inertial degree of $\mathfrak{p}$ in F_E/F is 3 since the Galois group is non-abelian. This corresponds to the last case of the table.

If $\mathfrak{p}\mathscr{O}_{F_P}$ factors as a product of two ideals $\mathfrak{p}_1\mathfrak{p}_2$, one of them has inertial degree 1 and the other has inertial degree 2. Since the inertial degree is multiplicative, the inertial degree of $\mathfrak{p}$ in F_E/F is 2 and we are in the second case.

The not so trivial case is the first one. Since F_E/F is Galois, $\mathfrak{p}\mathscr{O}_{F_E}$ has 3 or 6 prime factors. Assume

$$\mathfrak{p}\mathscr{O}_{F_E} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3. \tag{4.1.1}$$

Then it must be the case that (after relabeling the ideals if needed) if σ denotes one order three element in $\mathrm{Gal}(F_E/F)$, $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$ and $\sigma^2(\mathfrak{q}_1) = \mathfrak{q}_3$. Since the decomposition groups $D(\mathfrak{q}_i|\mathfrak{p})$ have order 2 and are conjugates to each other by powers of σ, they are disjoint and they are all the order 2 subgroups of S_3. Since F_P is a degree 2 subextension of F_E, it is the fixed field of an order 2 subgroup. Without loss of generality, assume F_P is the fixed field of $D(\mathfrak{q}_1|\mathfrak{p})$. If we intersect equation (4.1.1) with $\mathscr{O}_{F_P}$ we get

$$\mathfrak{p}\mathscr{O}_{F_P} = (\mathfrak{q}_1 \cap \mathscr{O}_{F_P})(\mathfrak{q}_2 \cap \mathscr{O}_{F_P})(\mathfrak{q}_3 \cap \mathscr{O}_{F_P}).$$

We are assuming that $(\mathfrak{q}_i \cap \mathscr{O}_{F_P}) \neq (\mathfrak{q}_j \cap \mathscr{O}_{F_P})$ if $i \neq j$. Let τ be the non trivial element in $D(\mathfrak{q}_1|\mathfrak{p})$, so τ acts trivially on F_P. In particular, τ fixes $\mathfrak{q}_2 \cap \mathscr{O}_{F_P}$ and $\tau(\mathscr{O}_{F_E}) = \mathscr{O}_{F_E}$ then $\tau(\mathfrak{q}_2) = \tau((\mathfrak{q}_2 \cap \mathscr{O}_{F_P})\mathscr{O}_{F_E}) = \mathfrak{q}_2$ which contradicts that $D(\mathfrak{q}_1|\mathfrak{p}) \cap D(\mathfrak{q}_2|\mathfrak{p}) = \{1\}$. □

Next we need to discard the C_3 case. Let $\mathfrak{m}_F$ be as described in step (1) of the algorithm, and $Cl(\mathscr{O}_F, \mathfrak{m}_F)$ be the ray class group. Suppose that $\overline{r_\Pi}$ has image isomorphic to C_3. Let χ be (one of) the cubic characters of $Cl(\mathscr{O}_F, \mathfrak{m}_F)$ corresponding to F_Π. Let $\{\chi_i\}_{i=1}^m$ be a basis of cubic characters of $Cl(\mathscr{O}_F, \mathfrak{m}_F)$. We look for prime ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ that are inert in F'_E or split completely in F_E (that is, they have order 1 or 2 in S_3 and in particular have even trace for the residual representation $\overline{r_E}$) and such that $\left\langle(\log(\chi_1(\mathfrak{p}_j)), \dots, \log(\chi_m(\mathfrak{p}_j)))\right\rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$. There exists such ideals by Tchebotarev's density Theorem. By Proposition 4.4, there exists an index i_0 such that $\chi(\mathfrak{p}_{i_0}) \neq 1$, hence $\mathrm{Tr}(\overline{r_\Pi}(\mathfrak{p}_{i_0})) \equiv 1 \pmod 2$ while $\mathrm{Tr}(\overline{r_E}(\mathfrak{p}_{i_0})) \equiv 0 \pmod 2$. Step (6) discards this case.

Once we know that $\overline{r_\Pi}$ has S_3 image with the same quadratic subfield as $\overline{r_E}$, we take F'_E as the base field and proceed in the same way as the previous case. This is done in steps (7) and (8).

At this point we already decided whether the two residual representations are isomorphic or not. If they are, we can apply Faltings-Serre method explained in the previous section. It implies computing all fields $\tilde{K}$ with Galois group $\mathrm{Gal}(\tilde{K}/F) \cong S_4 \times C_2$. We claim that it is enough to look for quadratic extensions $\tilde{K}$ of K unramified outside $\mathfrak{m}_K$ such that its normal closure is isomorphic to S_4 or $S_3 \times C_2$.

The claim comes from the fact that the group $S_4 \times C_2$ fits in the exact sequences

$$1 \to C_2 \times C_2 \to S_4 \times C_2 \to S_3 \times C_2 \to 1$$

and

$$1 \to C_2 \to S_4 \times C_2 \to S_4 \to 1.$$

Furthermore, every element of order 4 or 6 in $S_4 \times C_2$ maps to an element of order 4 in S_4 or to an element of order 6 on $S_3 \times C_2$ under the previous surjections. Then if we compute normal extensions of K with Galois group S_4 or $S_3 \times C_2$ and a prime element of order 4 or 6 in each one of them, this set of primes is enough to decide whether the representations are isomorphic or not. The advantage of considering these two extensions is that they are obtained as normal closure of quadratic extensions of K.

Let $\mathfrak{m}_K$ be a modulus in K invariant under the action of $\mathrm{Gal}(K/F)$. Then $\mathrm{Gal}(K/F)$ has an action on $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ and it induces an action on the set of characters of the group. Concretely, if ψ is a character in $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ and $\sigma \in \mathrm{Gal}(K/F)$, $\sigma.\psi = \psi \circ \sigma$.

LEMMA 4.10. *If ψ is a character of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ that corresponds to the quadratic extension $K[\sqrt{\alpha}]$ and $\sigma \in \mathrm{Gal}(K/F)$ then $\sigma^{-1}.\psi$ corresponds to $K[\sqrt{\sigma(\alpha)}]$.*

PROOF. The character is characterized by its value on non-ramified primes. Let $\mathfrak{p}$ be a non-ramified prime on $K[\sqrt{\alpha}]/K$. It splits in $K[\sqrt{\alpha}]$ if and only if $\psi(\mathfrak{p}) = 1$. If $\mathfrak{p}$ does not divide the fractional ideal α, this is equivalent to α being a square modulo $\mathfrak{p}$. But for $\sigma \in \mathrm{Gal}(K/F)$, α is a square modulo $\mathfrak{p}$ if and only if $\sigma(\alpha)$ is a square modulo $\sigma(\mathfrak{p})$, hence the extension $K[\sqrt{\sigma(\alpha)}]$ corresponds to the character $\sigma^{-1}.\psi$. □

PROPOSITION 4.11. *Let K/F be a Galois extension with $\mathrm{Gal}(K/F) \cong S_3$ and ψ a quadratic character of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$, with $\mathfrak{m}_K$ as above.*

(1) *The quadratic extension of K corresponding to ψ is Galois over F if and only if $\sigma.\psi = \psi$ for all $\sigma \in \mathrm{Gal}(K/F)$.*
(2) *The quadratic extension of K corresponding to ψ has normal closure isomorphic to S_4 if and only if the elements fixing ψ form an order 2 subgroup and $\psi \cdot (\sigma.\psi) = \sigma^2.\psi$, where σ is any order 3 element in $\mathrm{Gal}(K/F)$.*

PROOF. Let $K[\sqrt{\alpha}]$ be a quadratic extension of K. The normal closure (with respect to F) is the field

$$\tilde{K} = \prod_{\sigma \in \mathrm{Gal}(K/F)} K[\sqrt{\sigma(\alpha)}]$$

(where by the product we mean the smallest field containing all of them inside $\bar{F}$). In particular $\mathrm{Gal}(\tilde{K}/K)$ is an abelian 2-group. By the previous proposition, if $K[\sqrt{\alpha}]$ corresponds to the quadratic character ψ then the other ones correspond to the characters $\sigma.\psi$ where $\sigma \in \mathrm{Gal}(K/F)$.

The first assertion is clear. To prove the second one, the condition $(\psi)(\sigma.\psi) = \sigma^2\psi$ and ψ being fixed by an order 2 subgroup implies that $[\tilde{K} : K] = 4$. Hence the group $\mathrm{Gal}(\tilde{K}/F)$ fits in the exact sequence

$$1 \to C_2 \times C_2 \to \mathrm{Gal}(\tilde{K}/F) \to S_3 \to 1.$$

In particular $\mathrm{Gal}(\tilde{K}/F)$ is isomorphic to the semidirect product $S_3 \ltimes (C_2 \times C_2)$, with the action given by a morphism $\Theta : S_3 \to \mathrm{GL}_2(\mathbb{F}_2)$. Its kernel is a normal subgroup, hence it can be $\mathrm{GL}_2(\mathbb{F}_2)$ (i.e. the trivial action), $\langle\sigma\rangle$ (the order 3 subgroup) or trivial. The condition on the stabilizer of ψ forces the image of Θ to contain an order 3 element, hence the kernel is trivial. Up to inner automorphisms, there is a unique isomorphism from $\mathrm{GL}_2(\mathbb{F}_2)$ to itself (and morphisms that differ by an inner automorphism give isomorphic groups) hence $\mathrm{Gal}(\tilde{K}/F) \cong S_4$ as claimed. □

REMARK 4.12. On the S_4 case of the last proposition, the condition on the action of σ is necessary. Consider the extension $K = \mathbb{Q}[\xi_3, \sqrt[3]{2}]$ where ξ_3 is a primitive third root of unity. It is a Galois degree 6 extension of $\mathbb{Q}$ with Galois group S_3. Take as generators for the Galois group the elements σ, τ given by

$$\begin{array}{lcl} \sigma : \xi_3 \mapsto \xi_3 & \text{and} & \sigma : \sqrt[3]{2} \mapsto \xi_3\sqrt[3]{2} \\ \tau : \xi_3 \mapsto \xi_3^2 & \text{and} & \tau : \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{array}$$

The extension $K\left[\sqrt{1+\sqrt[3]{2}}\right]$ is clearly fixed by τ, but its normal closure has degree 8 over K since $\sqrt{1+\xi_3^2\sqrt[3]{2}}$ is not in the field $K\left[\sqrt{1+\sqrt[3]{2}}, \sqrt{1+\xi_3\sqrt[3]{2}}\right]$ as can be easily checked.

To compute all such extensions, we use Class Field Theory and Proposition 4.11. The first case is compute the $S_3 \times C_2$ extensions. A quadratic character χ is invariant under σ if and only if the character $\chi \cdot (\sigma.\chi)$ is trivial. If $\{\chi_i\}_{i=1}^n$ is a basis for the quadratic characters, $\chi = \prod_{i=1}^n \chi_i^{\varepsilon_i}$ for some ε_i. We are looking for exponents ε_i modulo 2 such that

$$\sum_{i=1}^n \varepsilon_i \log(\chi_i(\mathfrak{a})\chi_i(\sigma.\mathfrak{a})) = 0$$

for all ideals $\mathfrak{a}$. Since the characters are multiplicative, it is enough to check this condition on a basis. This is the system we consider in step (11) for an order 3 element σ of $\mathrm{Gal}(F_E/F)$. On step (12) we do the same for an order 2 element τ of $\mathrm{Gal}(F_E/F)$ and in step (13) we compute the intersection of the two subspaces. These characters give all $S_3 \times C_2$ extensions of F_E. On step (14), using Proposition 4.4 we compute prime ideals having order 6 on each such extension.

At last, we need to compute the quadratic extensions whose normal closure has Galois group isomorphic to S_4. Using the second part of Proposition 4.11, we need to compute quadratic characters χ such that $\chi(\sigma.\chi)(\sigma^2.\chi) = 1$ (where σ denotes an order three element of $\mathrm{Gal}(K/F)$) and also whose fixed subgroup under the action of $\mathrm{Gal}(K/F)$ has order 2. Let S denote the set of all such characters. Since σ does not act trivially on elements of S, we find that χ, $\sigma.\chi$ and $\sigma^2.\chi$ are three different elements of S that give the same normal closure. Then we can write S as a disjoint union of three sets. Furthermore, since σ acts transitively (by multiplication on the right) on the set of order 2 elements of S_3, we see that

$$S = V_\tau \cup V_{\tau\sigma} \cup V_{\tau\sigma^2}$$

where V_τ denotes the quadratic characters of S invariant under the action of τ and the union is disjoint. Hence each one of these sets is in bijection with all extensions $\tilde{K}$ of K. We compute one subspace and then use Proposition 4.4 on a basis of it to compute prime ideals of F having order 4 in each such extension. Note that the elements of order 4 correspond to prime ideals that are inert in any of the three extensions of K (corresponding to χ, $\sigma.\chi$ and $\sigma^2.\chi$) hence we consider not one prime above $\mathfrak{p} \subset \mathscr{O}_F$ but all of them. This is done in steps $(16) - (19)$.

4.2. Trivial residual image or residual image isomorphic to C_2. The first step is to decide if we can take L to be an extension of $\mathbb{Q}_2$ with residue field $\mathbb{F}_2$ so as to apply Livne's Theorem 3.3. Once this is checked, the algorithm is divided into two parts. Let $r_E, r_\Pi : \Gamma_F \to \mathrm{GL}_2(\mathbb{Z}_2)$ be given, with the residual image of r_E being either trivial or isomorphic to C_2. Steps (2) to (6) serve to the purpose of seeing whether r_Π has also trivial or C_2 residual image or not. Note that the output of step (6) does not say that the residual representations are actually the same, but that they have isomorphic semisimplifications (in this case it is equivalent to say that the traces are even). For example, there can be isogenous curves, one of which has trivial residual image and the other has C_2 residual image.

Suppose we computed the ideals of steps $(2) - (5)$ and $\overline{r_\Pi}$ has even trace at the Frobenius of these elements. We claim that r_Π has residual image either trivial or C_2. Suppose on the contrary that r_Π has residual image isomorphic to C_3. Let K/F be the cyclic extension of F corresponding (by Galois theory) to the kernel of $\overline{r_\Pi}$. This corresponds to a cubic character χ of $Cl(\mathscr{O}_F, \mathfrak{m}_F)$. An easy calculation shows that if $\mathfrak{p} \subset \mathscr{O}_F$ is a prime ideal not dividing $\mathfrak{m}_F$, then $\chi(\mathfrak{p}) = 1$ if and only if $\mathrm{Tr}(\overline{r_\Pi}(\mathrm{Frob}_\mathfrak{p})) = 0$. This implies that $\chi(\mathfrak{p}_j) = 1$ for each $j = 1, \ldots, m$. But χ is a non-trivial character, then by Proposition 4.4 we get a contradiction.

Similarly, suppose that the residual image of r_Π is S_3. Let K/F be the S_3 extension of F corresponding (by Galois theory) to the kernel of $\overline{r_\Pi}$, and K'/F its unique quadratic subextension. The extension K/K' corresponds to a cubic character χ of $Cl(\mathscr{O}_{K'}, \mathfrak{m}_{K'})$ and the proof follows the previous case.

Steps $(7) - (10)$ check if the representations are indeed isomorphic once we know that the traces are even using Theorem 3.3. We need to find a finite set of primes T, which will only depend on F, and check that the representations agree at those primes. In the algorithm and in the theorem, we identify the group $\mathrm{Gal}(F_S/F)$ with the group of quadratic characters of $Cl(\mathscr{O}_F, \mathfrak{m}_F)$. In step (8), we compute the image of $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(F_S/F)$ via this isomorphism and compute enough prime ideals so as to get a non-cubic set of $\mathrm{Gal}(F_S/F)$. Then the semisimplifications of the representations are isomorphic if and only if the traces at those primes agree.

4.3. Residual image isomorphic to C_3. The first step is to decide if we can take L to be an extension of $\mathbb{Q}_2$ with residue field $\mathbb{F}_2$. Once this is checked, we need to prove that the residual representation $\overline{r_\Pi}$ has image isomorphic to C_3. For doing this we start proving that it has no order 2 elements in its image. If such an element exists, there exists a degree 2 extension of F, unramified outside $2\mathfrak{n}_E\mathfrak{n}_\Pi\overline{\mathfrak{n}_\Pi}d_F$. We use Proposition 4.3 and class field theory to compute all such extensions. Once a basis of the quadratic characters is chosen, we apply Proposition 4.4 to find a set of ideals such that for any quadratic extension, (at least) one prime $\mathfrak{q}$ in the set is inert in it. Since the residual image is isomorphic to a subgroup of S_3, $\overline{r_\Pi}(\mathrm{Frob}_\mathfrak{q})$ has order exactly 2. In particular its trace is even. If $\mathrm{Tr}(\overline{r_\Pi}(\mathrm{Frob}_\mathfrak{p}))$ is odd at all primes, $\mathrm{im}(\overline{r_\Pi})$ contains no order 2 elements. Also since $\mathrm{Tr}(\mathrm{id}) \equiv 0 \pmod 2$ we see that $\overline{r_\Pi}$ cannot have trivial image hence its image is isomorphic to C_3. This is done in steps (2) to (5) of the algorithm.

To prove that $\overline{r_\Pi}$ factors through the same field as $\overline{r_E}$, we compute all cubic Galois extensions of F. This can be done using Class Field Theory again, and this explains the choice of the modulus in step (1), so as to be used for both quadratic and cubic extensions. Note that the characters χ and χ^2 give rise to the same field extension. If ψ_E denotes (one of) the cubic character corresponding to F_E, we extend it to a basis $\{\psi_E, \chi_i\}_{i=1}^m$ of the cubic characters of $Cl(\mathscr{O}_F, \mathfrak{m}_F)$ and find a set of prime ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ such that $\left\langle(\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j)))\right\rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$ and $\psi_E(\mathfrak{p}_j) = 1$ for all $1 \leqslant j \leqslant m'$.

If χ is a cubic character corresponding to F_Π, $\chi = \psi_E^\varepsilon \varkappa$, where $\varkappa = \prod_{i=1}^n \chi_i^{\varepsilon_i}$. If $\varkappa = 1$, then $\chi = \psi_E$ or ψ_E^2 and we are done. If not, by Proposition 4.4, there exists an index i_0 such that $\varkappa(\mathfrak{p}_{i_0}) \neq 1$. Furthermore, since $\psi_E(\mathfrak{p}_{i_0}) = 1$, $\chi(\mathfrak{p}_{i_0}) \neq 1$. Hence $\mathrm{Tr}(\overline{r_\Pi}(\mathfrak{p}_{i_0})) \equiv 1 \pmod 2$ and $\mathrm{Tr}(\overline{r_E}(\mathfrak{p}_{i_0})) \equiv 0 \pmod 2$.

At this point we already decided whether the two residual representations are isomorphic or not. If they are, we can apply Livne's Theorem 3.3 to the field F_E' which is the last step of the algorithm.

5. Examples

In this section we present three examples of elliptic curves over imaginary quadratic fields, one for each class of residual 2-adic image and show how the method works. The first publications comparing elliptic curves with modular forms over imaginary quadratic fields are due to Cremona and Whitley (see [**CW94**]), where they consider imaginary quadratic fields with class number 1. The study was continued by other students of Cremona. The examples we consider are taken from Lingham's

$\mathcal{N}\,\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_{\mathfrak{p}}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$
3	$\langle 2,\omega\rangle$	-2	$\langle 2,\omega+1\rangle$	1
25	$\langle 5\rangle$	-1		
49	$\langle 7\rangle$	-4		
29	$\langle 29,\omega+10\rangle$	0	$\langle 29,\omega+18\rangle$	-3
31	$\langle 31,\omega+7\rangle$	5	$\langle 31,\omega+23\rangle$	-4
41	$\langle 41,\omega+25\rangle$	12	$\langle 41,\omega+15\rangle$	9
47	$\langle 47,\omega+33\rangle$	9	$\langle 47,\omega+13\rangle$	6

TABLE 1. Values of $a_{\mathfrak{p}}$ used to prove modularity in the S_3 example.

Ph.D. thesis (see **[Lin05]**), who considered imaginary quadratic fields with class number 3.

All our computations were done using the PARI/GP system ([**PAR08**]). On the next section we present the commands used to check our examples so as to serve as a guide for further cases. The routines were written by the author together with Dieulefait and Pacetti, and can be downloaded from **[CNT]**, under the item "modularity".

5.1. Image isomorphic to S_3. Let $F = \mathbb{Q}[\sqrt{-23}]$ and $\omega = \frac{1+\sqrt{-23}}{2}$. Let E be the elliptic curve with equation

$$E : y^2 + \omega xy + y = x^3 + (1-\omega)x^2 - x$$

It has conductor $\mathfrak{n}_E = \bar{\mathfrak{p}}_2\mathfrak{p}_{13}$ where $\bar{\mathfrak{p}}_2 = \langle 2, 1-\omega\rangle$ and $\mathfrak{p}_{13} = \langle 13, 8+\omega\rangle$. There is an automorphic representation Π of level $\mathfrak{n}_\Pi = \bar{\mathfrak{p}}_2\mathfrak{p}_{13}$ and trivial character (corresponding to the form denoted by f_2 in **[Lin05]** table 7.1) which is the candidate to Let r_E be the 2-adic Galois representation attached to E. Its residual representation has image isomorphic to S_3 as can easily be checked by computing the extension F_E of F obtained adding the coordinates of the 2-torsion points. Using the routine `Setofprimes` we find that the set of primes of $\mathbb{Q}[\sqrt{-23}]$ dividing the rational primes $\{3, 5, 7, 29, 31, 41, 47\}$ is enough for proving that the residual representations are isomorphic and that the 2-adic representations are isomorphic as well. Note that the normal answer of the routine would be the set $\{3, 5, 7, 11, 19, 29, 31, 37\}$, but since some of these ideals have norm greater than 50, they are not in table 7.1 of **[Lin05]**. This justifies using some flags in the routine (as documented) to get our first list and prove modularity in this particular case. The values of the $a_{\mathfrak{p}}$ for these primes are listed in Table 1.

To prove that the answer is correct, we apply the algorithm described in section 1.1:

(1) Since 2 is unramified in $F/\mathbb{Q}$, the modulus is $\mathfrak{m}_F = 2^3 13\sqrt{-23}$.
(2) The ray class group is isomorphic to $C_{396} \times C_{12} \times C_2 \times C_2 \times C_2 \times C_2$. Using Remark 4.9 we find that the character ψ in the computed basis corresponds to χ_3, where $\{\chi_i\}$ is the dual basis of quadratic characters.

(3) The extended basis is $\{\psi, \chi_1, \chi_2, \chi_4, \chi_5, \chi_6\}$. Computing some prime ideals, we find that the set $\{\bar{\mathfrak{p}}_3, \mathfrak{p}_5, \bar{\mathfrak{p}}_{29}, \mathfrak{p}_{31}, \mathfrak{p}_{47}\}$ has the desired properties (using Remark 4.9 we know that the primes with inertial degree 3 are the ones in the third case).

(4) Table 1 shows that $\mathrm{Tr}(\overline{r_\Pi}(\mathrm{Frob}_\mathfrak{p}))$ is odd in all such primes $\mathfrak{p}$.

(5) The group of cubic characters has as dual basis for $Cl(\mathscr{O}_F, \mathfrak{m}_F)$ the characters $\{\chi_1, \chi_2\}$, i.e. $\chi_i(v_j) = \delta_{ij}\xi_3$, where ξ_3 is a primitive cubic root of unity. The ideals $\mathfrak{p}_3$ and $\mathfrak{p}_7$ are inert in the quadratic subextension of F_E and

$$\langle(\log(\chi_1(\mathfrak{p}_3)), \log(\chi_2(\mathfrak{p}_3))), (\log(\chi_1(\mathfrak{p}_7)), \log(\chi_2(\mathfrak{p}_7)))\rangle = (\mathbb{Z}/3\mathbb{Z})^2$$

(6) From Table 1 we see that $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_3}))$ is even, hence $\overline{r_\Pi}$ has image S_3 with the same quadratic subfield as $\overline{r_E}$.

(7) The field F'_E can be given by the equation $x^4 + 264 \cdot x^3 + 26896 \cdot x^2 + 1244416 \cdot x + 21958656$. The prime number 2 is ramified in F'_E, and factors as $2\mathscr{O}_{F'_E} = \mathfrak{p}_{2,1}^2\mathfrak{p}_{2,2}$. The prime number 13 is also ramified and factors as $13\mathscr{O}_{F'_E} = \mathfrak{p}_{13,1}^2\mathfrak{p}_{13,2}\mathfrak{p}_{13,3}$. The prime number 23 is ramified, but has a unique ideal dividing it in F'_E. The modulus to consider is $\mathfrak{m}_{F'_E} = \mathfrak{p}_{2,1}\mathfrak{p}_{2,2}\mathfrak{p}_{13,1}\mathfrak{p}_{13,2}\mathfrak{p}_{13,3}\mathfrak{p}_{23}$.

(8) $Cl(\mathscr{O}_{F'_E}, \mathfrak{m}_{F'_E}) \cong C_{792} \times C_{12} \times C_6 \times C_3$. We claim that $\psi_E = \chi_4$, where χ_i is the dual basis for cubic characters of $Cl(\mathscr{O}_{F'_E}, \mathfrak{m}_{F'_E})$. We know that $\mathfrak{p}_3$ is inert in F'_E hence $\psi_E(\mathfrak{p}_3) = 1$. The prime number 7 is inert in F'_E hence $\psi_E(\mathfrak{p}_7) = 1$; the prime 37 is inert in F, but splits as a product of two ideals in F'_E. Then $\psi_E(\mathfrak{p}_{37}) = 1$ in both ideals. There is a unique (up to squares) character vanishing in them, and this is ψ_E.

The basis $\{\psi_E, \chi_1, \chi_2, \chi_3\}$ extends $\{\psi_E\}$ to a basis of cubic characters. The point here is that the characters χ_i need not give Galois extensions over F. A character gives a Galois extension if and only if its modulus is invariant under the action of $\mathrm{Gal}(F'_E/F)$. The characters χ_1, χ_3, χ_4 do satisfy this property, hence the subgroup of cubic characters of $Cl(\mathscr{O}_{F'_E}, \mathfrak{m}_{F'_E})$ with invariant conductor has rank 3. A basis is given by $\{\psi_E, \chi_1, \chi_3\}$. If we evaluate χ_1 and χ_3 at the prime above $\mathfrak{p}_3$ and $\mathfrak{p}_7$ we see that they span the $\mathbb{Z}/3\mathbb{Z}$-module. We already compared the residual traces in these ideals, hence the two residual representations are indeed isomorphic.

(9) We compute an equation for F_E over $\mathbb{Q}$. From the ideal factorizations $2\mathscr{O}_{F_E} = \mathfrak{q}_{2,1}^2\mathfrak{q}_{2,2}^2\mathfrak{q}_{2,3}^2\mathfrak{q}_{2,4}^3$, $13\mathscr{O}_{F_E} = \mathfrak{q}_{13,1}^2\mathfrak{q}_{13,2}^2\mathfrak{q}_{13,3}^2\mathfrak{q}_{13,4}\mathfrak{q}_{13,5}$ and $23\mathscr{O}_{F_E} = \mathfrak{q}_{23,1}^2\mathfrak{q}_{23,2}^2\mathfrak{q}_{23,3}^2$ we take

$$\mathfrak{m}_{F_E} = \mathfrak{q}_{2,1}^5\mathfrak{q}_{2,2}^5\mathfrak{q}_{2,3}^5\mathfrak{q}_{2,4}^7\mathfrak{q}_{13,1}\mathfrak{q}_{13,2}\mathfrak{q}_{13,3}\mathfrak{q}_{13,4}\mathfrak{q}_{13,5}\mathfrak{q}_{23,1}\mathfrak{q}_{23,2}\mathfrak{q}_{23,3}$$

as the modulus and compute the ray class group $Cl(\mathscr{O}_{F_E}, m_{F_E})$. It has 18 generators (see the *GP Code* section).

(10) We compute the Galois group $\mathrm{Gal}(F_E/F)$, and choose an order 3 and an order 2 element from it.

(11) We compute the kernels of the system and find out that the kernel for the order 3 element has dimension 8.
(12) The kernel for the order 2 element has dimension 11.
(13) The intersection of the previous two subspaces has dimension 6. It is generated by the characters
$$\{\chi_1, \chi_2\chi_5, \chi_2\chi_3\chi_6\chi_7, \chi_3\chi_4\chi_9, \chi_{12}\chi_{13}\chi_{14}, \chi_8\chi_{10}\chi_{12}\chi_{15}\chi_{17}\}.$$
(14) The ideals above $\{3, 5, 11, 29, 31\}$ satisfy that their logarithms span the $\mathbb{Z}/2\mathbb{Z}$ vector space.
(15) The ideal above 11 is missing in table 7.1 of **[Lin05]** since it has norm 121, but we can replace it by the ideals above 47 which appears in Table 1. So we checked that the two representations agree in order 6 elements.
(16) The space of elements satisfying the condition in the order 3 element has dimension 10.
(17) The intersection of the two subspaces has dimension 5. A basis is given by the characters
$$\{\chi_1\chi_2\chi_4, \chi_1\chi_2\chi_6, \chi_3\chi_{10}\chi_{11}\chi_{14}, \chi_3\chi_{16}, \chi_1\chi_{10}\chi_{11}\chi_{12}\chi_{13}\chi_{17}\}.$$
(18) The prime ideals above $\{3, 7, 19, 29, 31\}$ do satisfy the condition, but since the prime 19 is inert in F, its norm is bigger than 50. Nevertheless, we can replace it by the primes above 41 which are in Table 1.
(19) Looking at Table 1 we find that the two representations are indeed isomorphic.

If the stronger version of Theorem 2.1 saying that the level of the Galois representation equals the level of the automorphic form is true, the set of primes to consider can be diminished removing the primes above 37 in the second set of primes.

5.2. Trivial residual image or image isomorphic to C_2. Let E be the elliptic curve over $F = \mathbb{Q}[\sqrt{-31}]$ with equation
$$E : y^2 + \omega xy = x^3 - x^2 - (\omega + 6)x,$$
where $\omega = \frac{1+\sqrt{-31}}{2}$. According to **[Lin05**, Table 5.1], the conductor of E is $\mathfrak{p}_2\mathfrak{p}_5$, where $\mathfrak{p}_2 = \langle 2, \omega\rangle$ and $\mathfrak{p}_5 = \langle 5, \omega + 1\rangle$. There is an automorphic representation Π of this level and trivial character (corresponding to the form denoted by f_1 in **[Lin05**, Table 7.4]) which is the candidate to correspond to E. Let r_E be the 2-adic Galois representation attached to E. Its residual representation has image isomorphic to C_2 as can easily be checked by computing the extension F_E of F obtained adding the coordinates of the 2-torsion points.

Using the routine `Setofprimes`, we find that the set
$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 47, 59, 67, 71, 89, 97, 101, 103, 107, 109, 149, 157, \\ 163, 191, 193, 211, 293, 311, 317, 359, 443, 577, 607, 617, 653, 691, 701\}$$
is enough for proving that the residual representations are isomorphic and that the 2-adic representations are isomorphic as well. The values of the $a_\mathfrak{p}$ for these primes are

$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_{\mathfrak{p}}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$	$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_{\mathfrak{p}}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$
3	$\langle 3\rangle$	-4			109	$\langle 109, 14+\omega\rangle$	12	$\langle 109, 94+\omega\rangle$	-10
7	$\langle 7, 2+\omega\rangle$	4	$\langle 7, 4+\omega\rangle$	2	149	$\langle 149, 38+\omega\rangle$	10	$\langle 149, 110+\omega\rangle$	10
11	$\langle 11\rangle$	10			157	$\langle 157, 17+\omega\rangle$	-14	$\langle 157, 139+\omega\rangle$	10
13	$\langle 13\rangle$	16			163	$\langle 163, 67+1\omega\rangle$	24	$\langle 163, 95+1\omega\rangle$	-20
17	$\langle 17\rangle$	-18			191	$\langle 191, 27+1\omega\rangle$	8	$\langle 191, 163+1\omega\rangle$	24
19	$\langle 19, 5+\omega\rangle$	-6	$\langle 19, 13+\omega\rangle$	0	193	$\langle 193, 55+1\omega\rangle$	-10	$\langle 193, 137+1\omega\rangle$	-2
23	$\langle 23\rangle$	-30			211	$\langle 211, 89+1\omega\rangle$	20	$\langle 211, 121+1\omega\rangle$	6
29	$\langle 29\rangle$	30			293	$\langle 293, 76+1\omega\rangle$	28	$\langle 293, 216+1\omega\rangle$	-14
41	$\langle 41, \omega+12\rangle$	-2	$\langle 41, \omega+28\rangle$	2	311	$\langle 311, 111+1\omega\rangle$	-32	$\langle 311, 199+1\omega\rangle$	0
47	$\langle 47, 21+\omega\rangle$	6	$\langle 47, 25+\omega\rangle$	-8	317	$\langle 317, 35+1\omega\rangle$	-6	$\langle 317, 281+1\omega\rangle$	-18
59	$\langle 59, 10+\omega\rangle$	-4	$\langle 59, 48+\omega\rangle$	0	359	$\langle 359, 158+1\omega\rangle$	22	$\langle 359, 200+1\omega\rangle$	-18
67	$\langle 67, 30+\omega\rangle$	12	$\langle 67, 36+\omega\rangle$	-2	443	$\langle 443, 66+1\omega\rangle$	-4	$\langle 443, 376+1\omega\rangle$	-20
71	$\langle 71, 26+\omega\rangle$	-8	$\langle 71, 44+\omega\rangle$	-8	577	$\langle 577, 217+1\omega\rangle$	32	$\langle 577, 359+1\omega\rangle$	-10
89	$\langle 89\rangle$	110			607	$\langle 607, 291+1\omega\rangle$	-8	$\langle 607, 315+1\omega\rangle$	48
97	$\langle 97, 19+\omega\rangle$	16	$\langle 97, 77+\omega\rangle$	-2	617	$\langle 617, 78+1\omega\rangle$	2	$\langle 617, 538+1\omega\rangle$	30
101	$\langle 101, 37+\omega\rangle$	10	$\langle 101, 63+\omega\rangle$	0	653	$\langle 653, 157+1\omega\rangle$	-18	$\langle 653, 495+1\omega\rangle$	-4
103	$\langle 103, 40+\omega\rangle$	0	$\langle 103, 62+\omega\rangle$	8	691	$\langle 691, 52+1\omega\rangle$	-20	$\langle 691, 638+1\omega\rangle$	28
107	$\langle 107, 20+\omega\rangle$	-4	$\langle 107, 86+\omega\rangle$	-6	701	$\langle 701, 221+1\omega\rangle$	-22	$\langle 701, 479+1\omega\rangle$	34

TABLE 2. Values of $a_{\mathfrak{p}}$ used to prove modularity in the C_2 example.

listed in Table 2 which was computed by Cremona (using some Magma code written by himself and Lingham) and sent to us in a private communication. He also checked that these values match the elliptic curve ones, which proves modularity in this case. To prove that the answer is correct, we apply the algorithm described on section 1.2:

(1) The primes above 41 and 47 prove that the residual representation of the automorphic form lies in $\mathrm{GL}_2(\mathbb{F}_2)$, because the values of $a_{\mathfrak{p}_{41}}, a_{\bar{\mathfrak{p}}_{41}}, a_{\mathfrak{p}_{47}}$ and $a_{\bar{\mathfrak{p}}_{47}}$ are $-2, 2, 6, -8$ respectively (see Table 2). The degree 4 extension of $\mathbb{Q}_2$ has equation $x^4 - 16x^3 + 252x^2 - 1504x + 2756$, and the prime 2 is totally ramified in this extension.

(2) The modulus is $\mathfrak{m}_F = 2^3 5\sqrt{-31}$, and the ray class group $Cl(\mathcal{O}_F, \mathfrak{m}_F) \cong C_{60} \times C_{12} \times C_2 \times C_2 \times C_2 \times C_2$.

(3) $-$ (5) There are 64 quadratic (including the trivial) extensions of F with conductor dividing $\mathfrak{m}_F$. We calculate each one, with the corresponding ray class group described in the algorithm; we pick a basis of cubic characters of each group, and evaluate them at each prime in $\{3, 7, 11, 13, 17, 19\}$. It turns out that this set is indeed enough for proving whether $\overline{r_\Pi}$ has residual image trivial or isomorphic to C_2.

(6) Since $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}})) \equiv 0 \pmod 2$ for the primes in the previous set (see **[Lin05]** table 7.1) we get that the residual image is trivial or isomorphic to C_2.

(7) $-$ (8) The set

$$\{3, 7, 11, 13, 17, 19, 23, 29, 47, 59, 67, 71, 89, 97, 101, 103, 107, 109, 149, 157, 163, \\ 191, 193, 211, 293, 311, 317, 359, 443, 577, 607, 617, 653, 691, 701\}$$

is enough. In order to see this, we must check that the Frobenius at all the primes of F above these ones cover $\mathrm{Gal}(F_S/F)\backslash\{\mathrm{id}\}$. We calculate a basis

$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_\mathfrak{p}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$	$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_\mathfrak{p}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$
3	$\langle 3\rangle$	-2			293	$\langle 293, 76+\omega\rangle$	-14	$\langle 293, 216+\omega\rangle$	-30
5	$\langle 5, 1+\omega\rangle$	-1	$\langle 5, 3+\omega\rangle$	3	349	$\langle 349, 83+\omega\rangle$	2	$\langle 349, 265+\omega\rangle$	18
7	$\langle 7, 2+\omega\rangle$	-5	$\langle 7, 4+\omega\rangle$	-3	379	$\langle 379, 61+\omega\rangle$	-28	$\langle 379, 317+\omega\rangle$	-12
11	$\langle 11\rangle$	10			431	$\langle 431, 205+\omega\rangle$	-36	$\langle 431, 225+\omega\rangle$	4
10	$\langle 13\rangle$	-10			521	$\langle 521, 64+\omega\rangle$	6	$\langle 521, 456+\omega\rangle$	6
17	$\langle 17\rangle$	-2			577	$\langle 577, 217+\omega\rangle$	-10	$\langle 577, 359+\omega\rangle$	-42
19	$\langle 19, 5+\omega\rangle$	-7	$\langle 19, 13+\omega\rangle$	3	607	$\langle 607, 291+\omega\rangle$	-8	$\langle 607, 315+\omega\rangle$	40
23	$\langle 23\rangle$	-10			653	$\langle 653, 157+\omega\rangle$	-30	$\langle 653, 495+\omega\rangle$	50
29	$\langle 29\rangle$	-10			839	$\langle 839, 252+\omega\rangle$	32	$\langle 839, 586+\omega\rangle$	48
37	$\langle 37\rangle$	-38			857	$\langle 857, 109+\omega\rangle$	-10	$\langle 857, 747+\omega\rangle$	22
41	$\langle 41, 12+\omega\rangle$	-9	$\langle 41, 28+\omega\rangle$	-1	1031	$\langle 1031, 101+\omega\rangle$	-24	$\langle 1031, 929+\omega\rangle$	-24
43	$\langle 43\rangle$	-18			1063	$\langle 1063, 172+\omega\rangle$	-36	$\langle 1063, 890+\omega\rangle$	20
47	$\langle 47, 21+\omega\rangle$	0	$\langle 47, 25+\omega\rangle$	0	1117	$\langle 1117, 465+\omega\rangle$	-50	$\langle 1117, 651+\omega\rangle$	-18
53	$\langle 53\rangle$	42			1303	$\langle 1303, 222+\omega\rangle$	40	$\langle 1303, 1080+\omega\rangle$	-56
59	$\langle 59, 10+\omega\rangle$	7	$\langle 59, 48+\omega\rangle$	-3	1451	$\langle 1451, 142+\omega\rangle$	-52	$\langle 1451, 1308+\omega\rangle$	-20
67	$\langle 67, 30+\omega\rangle$	-8	$\langle 67, 36+\omega\rangle$	0	1493	$\langle 1493, 382+\omega\rangle$	-14	$\langle 1493, 1110+\omega\rangle$	-30
71	$\langle 71, 26+\omega\rangle$	1	$\langle 71, 44+\omega\rangle$	-9	1619	$\langle 1619, 577+\omega\rangle$	28	$\langle 1619, 1041+\omega\rangle$	-52
73	$\langle 73\rangle$	2			1741	$\langle 1741, 727+\omega\rangle$	74	$\langle 1741, 1013+\omega\rangle$	26
79	$\langle 79\rangle$	70			2003	$\langle 2003, 141+\omega\rangle$	-36	$\langle 2003, 1861+\omega\rangle$	-20
89	$\langle 89\rangle$	-50			2153	$\langle 2153, 404+\omega\rangle$	30	$\langle 2153, 1748+\omega\rangle$	30
109	$\langle 109, 14+\omega\rangle$	-13	$\langle 109, 94+\omega\rangle$	7	2333	$\langle 2333, 571+\omega\rangle$	94	$\langle 2333, 1761+\omega\rangle$	-34
127	$\langle 127\rangle$	-254			2707	$\langle 2707, 1053+\omega\rangle$	68	$\langle 2707, 1653+\omega\rangle$	-60
131	$\langle 131, 60+\omega\rangle$	4	$\langle 131, 70+\omega\rangle$	4	2767	$\langle 2767, 769+\omega\rangle$	-40	$\langle 2767, 1997+\omega\rangle$	8
149	$\langle 149, 38+\omega\rangle$	18	$\langle 149, 110+\omega\rangle$	2	2963	$\langle 2963, 1055+\omega\rangle$	0	$\langle 2963, 1907+\omega\rangle$	24
173	$\langle 173, 41+\omega\rangle$	10	$\langle 173, 131+\omega\rangle$	-6	3119	$\langle 3119, 665+\omega\rangle$	72	$\langle 3119, 2453+\omega\rangle$	-8
193	$\langle 193, 55+\omega\rangle$	11	$\langle 193, 137+\omega\rangle$	-21	3373	$\langle 3373, 857+\omega\rangle$	10	$\langle 3373, 2515+\omega\rangle$	90
227	$\langle 227, 106+\omega\rangle$	-12	$\langle 227, 120+\omega\rangle$	20	3767	$\langle 3767, 513+\omega\rangle$	32	$\langle 3767, 3253+\omega\rangle$	-80
283	$\langle 283, 47+\omega\rangle$	-20	$\langle 283, 235+\omega\rangle$	-20					

TABLE 3. Values of $a_\mathfrak{p}$ used to prove modularity in the C_3 example.

$\{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5\}$ for the quadratic characters of $Cl(\mathscr{O}_F, \mathfrak{m}_F)$, and compute, for $\mathfrak{p}$ a prime of F above one of these primes, $(\log\psi_1(\mathfrak{p}), \dots, \log\psi_5(\mathfrak{p}))$. We simply check that this set of coordinates has 63 elements, so the primes we listed are enough.

REMARK 5.1. We apply our routine to the curve over $\mathbb{Q}[\sqrt{-3}]$ of conductor $\left(\frac{17+\sqrt{-3}}{2}\right)$ considered by Taylor and got the same set of primes needed to prove modularity, as expected.

5.3. Image isomorphic to C_3**.** Let $F = \mathbb{Q}[\sqrt{-31}]$ and $\omega = \frac{1+\sqrt{-31}}{2}$. Let E be the elliptic curve with equation

$$E : y^2 = x^3 - x^2 + (3-\omega)x - 3.$$

It has conductor $\mathfrak{n}_E = \mathfrak{p}_2^3\bar{\mathfrak{p}}_2^2$ where $\mathfrak{p}_2 = \langle 2, \omega\rangle$. There is an automorphic representation Π of this level and trivial character (corresponding to the form denoted by f_5 in **[Lin05]** table 7.4) which is the candidate to correspond to E. Let r_E be the 2-adic Galois representation attached to E. Its residual representation has image isomorphic to C_3 as can easily be checked by computing the extension F_E of F obtained adding the coordinates of the 2-torsion points.

Using the GP routine `Setofprimes`, we find that the set of primes of $\mathbb{Q}[\sqrt{-31}]$ above

$$\{3,5,7,11,13,17,19,23,29,37,41,43,47,53,59,67,71,73,79,89,109,127,131,149,$$

$$173,193,227,283,293,349,379,431,521,577,607,653,839,857,1031,1063,1117,$$

$$1303,1451,1493,1619,1741,2003,2153,2333,2707,2767,2963,3119,3373,3767\}$$

is enough for proving that the residual representations are isomorphic and that the 2-adic representations are isomorphic as well. The values of the $a_{\mathfrak{p}}$ for these primes are listed in Table 3 which was computed by Cremona (using some Magma code written by himself and Lingham) and sent to us on a private communication. He also checked that these values match the elliptic curve ones, which proves modularity in this case. To prove that the answer is correct, we apply the algorithm described in section 1.3:

(1) The primes above 131 and 149 prove that the residual representation of the automorphic form lies in $\mathrm{GL}_2(\mathbb{F}_2)$, because the values of $a_{\mathfrak{p}_{131}}, a_{\bar{\mathfrak{p}}_{131}}, a_{\mathfrak{p}_{149}}$ and $a_{\bar{\mathfrak{p}}_{149}}$ are $4,4,18,2$ respectively. They satisfy the hypothesis of Theorem 4.1 and the degree 4 extension of $\mathbb{Q}$ obtained has equation $x^4-28x^3+684x^2-6832x+24992$, where the prime 2 factors as the product of two ramified primes.
(2) Since 2 is unramified in $F/\mathbb{Q}$, the modulus is $\mathfrak{m}_F=2^3.\sqrt{-31}$. We compute the ray class group and find that $Cl(\mathscr{O}_F,\mathfrak{m}_F)\cong C_{30}\times C_6\times C_2\times C_2$.
(3) The group of cubic characters has as dual basis for $Cl(\mathscr{O}_F,\mathfrak{m}_F)$ the characters $\{\chi_1,\chi_2\}$. On the routine basis, the cubic character (up to squares) that correspond to F_E is χ_1.
(4) Let $\{\chi_1,\dots,\chi_4\}$ be a set of generators of the order two characters of $Cl(\mathscr{O}_F,\mathfrak{m}_F)$ with respect to the previous isomorphism. By computing their values at prime ideals of $\mathscr{O}_F$ we found that the set $C=\{\mathfrak{p}_5,\bar{\mathfrak{p}}_5,\mathfrak{p}_7,\bar{\mathfrak{p}}_7\}$ satisfies the desired properties.
(5) The traces of the Frobenius at these primes are odd (see Table 3). Hence the residual image is isomorphic to C_3.
(6) Since there is only one other cubic character (χ_2), it turns out that $\chi_1(\mathfrak{p}_3)=1$, but $\chi_2(\mathfrak{p}_3)\neq 0$. Since $\mathrm{Tr}(r_\Pi(\mathrm{Frob}_{\mathfrak{p}_3}))\equiv\mathrm{Tr}(r_E(\mathrm{Frob}_{\mathfrak{p}_3}))\pmod 2$, the two residual representations are isomorphic.
(7) As in the previous example, Livne's method implies that the primes above the primes in the set

$$\{3,5,7,11,13,17,19,23,29,37,41,43,47,53,59,67,71,73,79,89,109,127,131,149,$$
$$173,193,227,283,293,349,379,431,521,577,607,653,839,857,1031,1063,1117,$$
$$1303,1451,1493,1619,1741,2003,2153,2333,2707,2767,2963,3119,3373,3767\}$$

are enough to prove modularity.

6. GP Code

In this section we show how to compute the previous examples with our routines and the outputs.

6.1. Image S_3.

```
? read(routines);
? F=bnfinit(w^2-w+6);
? Setofprimes(F,[w,1-w,1,-1,0],[2,13])
Case = S_3
Class group of F:  [396, 12, 2, 2, 2, 2]
Primes for discarding other quadratic extensions:
[3, 5, 11, 29, 31]
Primes discarding C_3 case:  [3, 7]
The ray class group for F_E' is  [792, 12, 6, 3]
Cubic character on F_E' basis:  [0; 0; 0; 1]
Primes proving C_3 extension of F_E':  [3, 7, 37]
Class group of K:  [2376, 12, 12, 12, 4, 4, 4, 4,
4, 2, 2, 2, 2, 2, 2, 2, 2, 2]
%3 = [3, 5, 7, 11, 19, 29, 31, 37]
```

6.2. Image isomorphic to C_2 or trivial.

```
? read(routines);
? F=bnfinit(w^2-w+8);
? Setofprimes(F,[w,-1,0,-w-6,0],[2,5])
Case = C_2 or trivial
Primes for proving that the residual representation lies
on F_2: [41, 47]
Class group of F:  [60, 12, 2, 2, 2, 2]
There are 64 subgroups of Cl_F of index <= 2
Primes proving C_2 or trivial case [3, 7, 11, 13, 17, 19]
Livne's method output:[3, 7, 11, 13, 17, 19, 23, 29, 47,
59, 67, 71, 89, 97, 101, 103, 107, 109, 149, 157, 163, 191,
193, 211, 293, 311, 317, 359, 443, 577, 607, 617, 653, 691,
701]
%3 = [3, 7, 11, 13, 17, 19, 23, 29, 41, 47, 59, 67, 71, 89,
97, 101, 103, 107, 109, 149, 157, 163, 191, 193, 211, 293,
311, 317, 359, 443, 577, 607, 617, 653, 691, 701]
```

6.3. Trivial residual image or image isomorphic to C_3.

```
? read(routines);
? F=bnfinit(w^2-w+8);
? Setofprimes(F,[0,-1,0,3-w,-3],[2])
Case = C_3
Primes for proving that the residual representation lies
```

```
on F_2: [131, 149]
Class group of F:  [30, 6, 2, 2]
Primes proving C_3 image:  [131, 149, 5, 7]
Cubic character on F basis:  [1; 0]
Primes proving C_3 extension of F_E':  [3]
Livne's method output:[3, 5, 7, 11, 13, 17, 19, 23, 29, 37,
41, 43, 47, 53, 59, 67, 71, 73, 79, 89, 109, 127, 131, 149,
173, 193, 227, 283, 293, 349, 379, 431, 521, 577, 607, 653,
839, 857, 1031, 1063, 1117, 1303, 1451, 1493, 1619, 1741,
2003, 2153, 2333, 2707, 2767, 2963, 3119, 3373, 3767]
%3 = [3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43, 47, 53,
59, 67, 71, 73, 79, 89, 109, 127, 131, 149, 173, 193, 227,
283, 293, 349, 379, 431, 521, 577, 607, 653, 839, 857, 1031,
1063, 1117, 1303, 1451, 1493, 1619, 1741, 2003, 2153, 2333,
2707, 2767, 2963, 3119, 3373, 3767]
```

Bibliography

[Ast94] *Périodes p-adiques*, Société Mathématique de France, Paris, 1994, Papers from the seminar held in Bures-sur-Yvette, 1988, Astérisque No. 223 (1994).

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[BH07] Tobias Berger and Gergely Harcos, *l-adic representations associated to modular forms over imaginary quadratic fields*, Int. Math. Res. Not. IMRN (2007), no. 23, Art. ID rnm113, 16.

[BLGG11] Thomas Barnet-Lamb, Toby Gee, and David Geraghty, *The Sato-Tate conjecture for Hilbert modular forms*, J. Amer. Math. Soc. **24** (2011), no. 2, 411–469.

[BLGGT10] T. Barnet-Lamb, T. Gee, D. Geraghty, and R. Taylor, *Potential automorphy and change of weight*, preprint, 2010.

[BLGHT] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, P.R.I.M.S., to appear.

[Car10] Ana Caraiani, *Local-global compatibility and the action of monodromy on nearby cycles*, preprint, 2010.

[Cas74] W. Casselman, *Introduction to the theory of admissible representations of p-adic groups*, preprint, 1974.

[CDT99] Brian Conrad, Fred Diamond, and Richard Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[CH09] G. Chenevier and M. Harris, *Construction of automorphic Galois representations, II*, 2009, preprint, 2009.

[CHLa] L. Clozel, M. Harris, and J.-P. Labesse, *Construction of automorphic Galois representations, I*, chapter in [CHLN].

[CHLb] ———, *Endoscopic transfer*, chapter in [CHLN].

[CHLN] L. Clozel, M. Harris, J.-P. Labesse, and B.C. Ngô (eds.), *Stabilization of the trace formula, Shimura varieties, and arithmetic applications. Volume 1: On the stabilization of the trace formula*, in preparation.

[CHT08] L. Clozel, M. Harris, and R. Taylor, *Automorphy for some ℓ-adic lifts of automorphic* mod ℓ *Galois representations*, Publ. Math., Inst. Hautes Étud. Sci. **108** (2008), 1–181.

[Clo90] Laurent Clozel, *Motifs et formes automorphes: applications du principe de fonctorialité*, Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988), Perspect. Math., vol. 10, Academic Press, Boston, MA, 1990, pp. 77–159.

[CNT] *Computational number theory*, `http://www.ma.utexas.edu/users/villegas/cnt/`.

[Coh00] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.

[Cre84] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), no. 3, 275–324.

[Cre92] ———, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2) **45** (1992), no. 3, 404–416.

[CSS97] Gary Cornell, Joseph H. Silverman, and Glenn Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer-Verlag, New York, 1997, Papers from the Instructional Conference on

Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[CW94] J. E. Cremona and E. Whitley, *Periods of cusp forms and elliptic curves over imaginary quadratic fields*, Math. Comp. **62** (1994), no. 205, 407–429.

[DGP10] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti, *Proving modularity for a given elliptic curve over an imaginary quadratic field*, Math. Comp. **79** (2010), no. 270, 1145–1170.

[Gue] Lucio Guerberoff, *Modularity lifting theorems for Galois representations of unitary type*, Compositio Math., to appear.

[HST93] Michael Harris, David Soudry, and Richard Taylor, *l-adic representations associated to modular forms over imaginary quadratic fields. I. Lifting to* $\mathrm{GSp}_4(\mathbf{Q})$, Invent. Math. **112** (1993), no. 2, 377–411.

[HT] M. Harris and R. Taylor, Manuscript 1998-2003.

[HT01] ———, *The geometry and cohomology of some simple Shimura varieties*, Annals of Mathematics Studies, vol. 151, Princeton University Press, Princeton, NJ, 2001, With an appendix by V. G. Berkovich.

[Kis09] Mark Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180.

[Lab] J.-P. Labesse, *Changement de base CM et séries discrètes*, chapter in [CHLN].

[Lin05] Mark Lingham, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph.D. thesis, University of Nottingham, October 2005, Available from `http://www.warwick.ac.uk/staff/J.E.Cremona/theses/index.html`.

[Liv87] Ron Livné, *Cubic exponential sums and Galois representations*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 247–261.

[Min] A. Minguez, *Unramified representations of unitary groups*, chapter in [CHLN].

[MW89] C. Mœglin and J.-L. Waldspurger, *Le spectre résiduel de* $\mathrm{GL}(n)$, Ann. Sci. École Norm. Sup. (4) **22** (1989), no. 4, 605–674.

[PAR08] The PARI Group, Bordeaux, *Pari/gp, version* `2.4.3`, 2008, available from `http://pari.math.u-bordeaux.fr/`.

[Rod82] François Rodier, *Représentations de* $\mathrm{GL}(n, k)$ *où k est un corps p-adique*, Bourbaki Seminar, Vol. 1981/1982, Astérisque, vol. 92, Soc. Math. France, Paris, 1982, pp. 201–218.

[Sch06] Matthias Schütt, *On the modularity of three Calabi-Yau threefolds with bad reduction at 11*, Canad. Math. Bull. **49** (2006), no. 2, 296–312.

[Ser66] Jean-Pierre Serre, *Groupes de Lie l-adiques attachés aux courbes elliptiques*, Les Tendances Géom. en Algébre et Théorie des Nombres, Éditions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 239–256.

[Ser68] ———, *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ser85] ———, *Résumé des cours de 1984-1985*, Annuaire du Collège de France (1985), 85–90.

[Ser95] ———, *Representaions lineaires sur des anneaux locaux, d'apres carayol*, Publ. Inst. Math. Jussieu **49** (1995).

[Shi11] S.W. Shin, *Galois representations arising from some compact Shimura varieties*, Ann. of Math. (2) **173** (2011), no. 3, 1645–1741.

[Tat79] J. Tate, *Number theoretic background*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 3–26.

[Tay94] Richard Taylor, *l-adic representations associated to modular forms over imaginary quadratic fields. II*, Invent. Math. **116** (1994), no. 1-3, 619–643.

[Tay08] R. Taylor, *Automorphy for some ℓ-adic lifts of automorphic* mod ℓ *Galois representations. II*, Publ. Math., Inst. Hautes Étud. Sci. **108** (2008), 183–239.

[Tho10] Jack Thorne, *On the automorphy of l-adic Galois representations with small residual image*, preprint, 2010.

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[TY07] Richard Taylor and Teruyoshi Yoshida, *Compatibility of local and global Langlands correspondences*, J. Amer. Math. Soc. **20** (2007), no. 2, 467–493 (electronic).

[Vig96] Marie-France Vignéras, *Représentations l-modulaires d'un groupe réductif p-adique avec $l \neq p$*, Progress in Mathematics, vol. 137, Birkhäuser Boston Inc., Boston, MA, 1996.

[Vig98] ———, *Induced R-representations of p-adic reductive groups*, Selecta Math. (N.S.) **4** (1998), no. 4, 549–623.

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Zel80] A. V. Zelevinsky, *Induced representations of reductive $\mathfrak{p}$-adic groups. II. On irreducible representations of* $\mathrm{GL}(n)$, Ann. Sci. École Norm. Sup. (4) **13** (1980), no. 2, 165–210.